MILITARY INTELLIGENCE LAW

Subcourse Number IT0466

EDITION C

US Army Intelligence Center
Fort Huachuca, AZ 85613-7000

6 Credit Hours

Edition Date: April 1998

SUBCOURSE OVERVIEW

This subcourse is designed to provide you with a working knowledge of the legal restrictions placed upon the collection of intelligence by AR 381-10 and other applicable laws and regulations.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time the subcourse was prepared.

In your own work situation, always refer to the latest publications.

The words "he", "him", and "men", when used in this publication, represent both the masculine and feminine genders unless otherwise stated.

TERMINAL LEARNING OBJECTIVE

ACTION:	You will be able to determine the legal ramifications impacting upon Counterintelligence (CI) investigations and implement the provisions of the Freedom of Information Act (FOIA), the Private Act, Executive Order (EO) 12333, and Army Regulations (AR) 381-10 and 381-20.
CONDITIONS:	You will be able to apply current intelligence law restrictions to all US Army counterintelligence investigations during peacetime and wartime.
STANDARDS:	You will conduct a counterintelligence investigation in accordance with the legal restrictions stated in **AR 381-10**, **AR 381-20**, and **EO 12333**.

TABLE OF CONTENTS

APPENDIX H: Acronyms

LESSON 1

LEGAL RAMIFICATIONS OF CI INVESTIGATIONS

CRITICAL TASKS: **NONE.**

OVERVIEW

LESSON DESCRIPTION

In this lesson, you will learn the limits of military jurisdiction and crimes of national security that are of interest to the CI agent. In addition, you will review the procedures for processing physical evidence and the rules of admitting evidence in a judicial proceeding.

TECHNICAL LEARNING OBJECTIVE:

TASKS: Be able to discuss rules of evidence, explain the limitations of military jurisdiction, define each of the national security crimes, and describe how to safeguard physical evidence. Be able to discuss rules of evidence, explain the limitations of military jurisdiction, define each of the national security crimes, and describe how to safeguard physical evidence.

CONDITIONS: You will be given narrative information pertaining to legal ramifications of CI investigations during both peacetime and wartime.

STANDARDS: You will analyze a CI investigation for potential legal impediments in accordance with the provisions of AR 381-10, AR 381-20, and EO 12333.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 380-5.
AR 380-67.
AR 381-10.
AR 381-20.
AR 600-10.
AR 600-31.
AR 600-37.
AR 600-40.
FM 19-20.
FM 34-60.

INTRODUCTION

As a Counterintelligence (CI) Agent involved in highly sensitive investigations, you must be thoroughly knowledgeable of both the military and civilian concepts of jurisdiction as defined by the Court of Military Appeals and the US Supreme Court. Although not required to be a subject matter expert, you are nevertheless required to have the basic skills necessary to collect and present evidence. In addition, you must be aware of the provisions of the Delimitations Agreement and how they apply to all phases of an investigation. An effective agent is one who has a thorough knowledge of all the basis legal ramifications.

This lesson has two parts:

Part A: Military Jurisdiction.

Part B: CI Investigations within the Military Jurisdiction System.

After each part, there is a practice exercise. Answer all the questions on each practice exercise and check your answers. Do NOT go on until you answer all the questions correctly.

PART A: MILITARY JURISDICTION

In this part of Lesson 1, you will learn:

* The definition of jurisdiction.

* The definition of military jurisdiction.

* The concept and historical background of military jurisdiction as it is currently interpreted.

* The categories of persons subject to military jurisdiction.

JURISDICTION.

As it is used in military law, jurisdiction is the right, power, or authority to administer justice. It refers to the categories of persons and offenses, as well as the extent or territory over which the right, power, or authority is exercised.

MILITARY JURISDICTION.

Military jurisdiction for the US military was defined by the US Constitution and has been interpreted by the US Supreme Court in a series of decisions.

Constitutional Provisions.

A system of military justice is specifically provided for in the Constitution. Article 1 of the Constitution provides, in part, that Congress has the power "to make Rules for the Government and Regulations of the land and naval forces". It further provides that Congress has the power "to make all laws which shall be necessary and proper for carrying into Execution the foregoing Powers..." These provisions indicate an awareness of the need for the military to have a system of procedural rules and regulations, and protections different from those prescribed by Article III of the Constitution.

In cases not arising in "the land and naval forces," an accused is entitled to "the benefit of an indictment by a grand jury" and a "trial by jury" as guaranteed by the Sixth Amendment of Article III of the Constitution. The Fifth Amendment, however, specifically exempts "cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger", from the requirement of prosecution by indictment.

The powers granted to the Congress mentioned above are the source of military law which provide for the creation of a system of military jurisdiction over personnel serving in the armed forces.

Limits of Military Jurisdiction in Cases Related to Military Service Members. There was no real question of the military's jurisdiction over its members and matters relating to military justice for more than 100 years (from 1863 to 1969). During this period, it was generally assumed military status was sufficient basis for the exercise of military jurisdiction over an accused. In 1969, however the US Supreme Court ruled in the case of O'Callahan V. Parker, 395 US 258 (1969), that offenses that were not service connected nor of military significance were not triable by military courts. As a result of that decision, military members that were charged with crimes recognized in a civilian court, of no military significance, and not service connected, were to be the constitutional rights of indictment by a grand jury and trial by a petit jury found in a civilian court. The majority opinion expressed concern over the lack of constitutional protection in military courts. This decision served as the basis for defining military court-martial jurisdiction until the landmark case of US v. Solorio, 107 S. Ct. 2924 (1987), which was decided in July 1987.

Solorio was charged with numerous sex offenses involving females under the age of 16, each of whom was the daughter of a fellow Coast Guardsman. Fourteen specifications of alleged misconduct took place of Juneau, Alaska (off-post) while seven specifications took place at Governor's Island New York (on-post). Solorio contested jurisdiction over the Alaskan offenses. The lower court dismissed the off-post offenses as not being connected to the service and therefore, not within the jurisdiction of the court. The Coast Guard appealed. Subsequent to the Court of Military Appeals' ruling that the lower court had jurisdiction over all offenses. Solorio petitioned the US Supreme Court. Chief Justice Rehnquist delivered the opinion for the majority. The Court held that military jurisdiction depended entirely on the status of the accused as a member of the Armed Forces. In so holding, the O'Callahan test for service connection was abandoned. The power of Congress to make rules for land and naval forces enables Congress to balance the needs of military against the rights of the soldier. Arguably, the Manual for Court-Martial, 1984, prescribed constitutional protection for the military accused that no longer supported the O'Callahan rationale for trying a soldier in a civilian court. In addition, as the Court commented, the civil courts are "ill-equipped" to establish policies regarding matters of military concern.

The net result of this recent case was to establish that the jurisdiction of the military court extends to any criminal act committed by a service member no matter where, when or for what purposes, the crime occurred.

Limits of Military Jurisdiction Over Civilians.

However, the trend in recent Supreme Court decisions has been to limit the scope of military jurisdiction. In 1955, the Supreme Court rendered such a decision in United States ex rel.Toth v. Quarles. In Toth, the accused was a civilian who had severed all connections with the military.

He was arrested by Air Force authorities and returned to Korea to stand trial by court-martial on charge of murder arising from an incident that occurred while he was on active duty and stationed in Korea. In Toth, the Supreme Court held that "Congress cannot subject civilians like Toth to trial by court-martial. They, like other civilians "the court noted, "are entitled to have a benefit of safeguards afforded those tried in the regular courts authorized by Article III of the Constitution."

The effect of the decision in Toth was to deny the military jurisdiction over service members who had severed all connections from the military for offenses committed while serving on active duty.

Peacetime Jurisdiction. The Army has court-martial authority over US Military personnel. With the enactment of the Uniform Code of Military Justice (UCMJ), Congress exposed certain types of civilians to trial by court-martial for offenses committed overseas. For example, Article 2(11) of the UCMJ specifically provided for the exercise of military jurisdiction over "person serving with, employed by, or accompanying the armed forces outside the United States..."

Attempts by the military to try civilians by court-martial under the provisions of Article 2(11) of the Codes, however, were not successful. The first in a number of decisions prohibiting the practice was rendered in 1957. At that time, the Supreme Court held the military did not have jurisdiction to try two American service wives for capital offenses committed overseas.

In Reid v. Covert, the wife of an Air Force sergeant stationed in England was tried by general court-martial and convicted of murdering her husband. In Kinsella v. Kruegner, a companion case, the accused was the wife of an Army officer stationed in Japan. Like Mrs. Covert, she was charged with the murder of her husband and was tried and convicted by general court-martial on the charge.

In both cases, the women filed writs of habeas corpus contending Article 2(11) of the UCMJ was unconstitutional. The Supreme Court agreed with petitioners. The court held the wives of servicemen "could not constitutionally be tried by the military authorities" for capital offenses committed overseas. A majority of the court determined that, as civilians charged with capital offenses in peacetime. the accused were entitled to trial in a civilian court under the procedural safeguards guaranteed by the Bill of Rights.

The court's decisions in these two cases caused others to question jurisdiction over civilian dependents committing noncapital offenses overseas. It also raised questions on whether the military could exercise jurisdiction over civilian employees of the armed forces committing capital and noncapital offenses overseas.

In 1960, in Grisham v. Hagan, the Supreme Court applied the reasoning set forth in Reid v. Convert and held that the military did not have jurisdiction to court-martial a civilian Army employee for a capital offense committed overseas during peacetime. In Grisham, the accused was a civilian employed by the

US Army in France. He was tried by general court-martial for premeditated murder and sentenced to life imprisonment.

The accused petitioned for a writ of habeas corpus alleging, in part, that Article 2(11) was unconstitutional as applied to him, because Congress lacked the power to deprive him of a civil trial affording all of the protections of Article III and the Fifth Amendment of the Constitution.

In effect, Grisham argued that, as a civilian defendant, he was entitled to the Constitutional protections granted to those tried by civilian courts. In Grisham, the Supreme Court determined civilian employees are entitled to trial by jury, just as civilian dependents are. Accordingly, it held the military did not have jurisdiction to try the accused for a capital offense committed overseas in peacetime.

In Kinsella v. United States ex rel. Singleton, 80 S. Ct. 297 also decided in 1960, the accused was Mrs. Dial a wife of a soldier stationed in Germany. She and her husband pled guilty in a trial by court-martial to charges of involuntary manslaughter in the death of one of their children. Mrs. Dial later appealed her conviction on the grounds of Article 2(11) of the Code, authorizing prosecution of court-martial trials of persons accompanying the armed forces outside the US, was unconstitutional when applied to civilian dependents charged with noncapital offenses.

In Kinsella, the Supreme Court held the military did not have jurisdiction over civilian dependents charged with noncapital and capital offenses. The court stated, in addition, that the test of jurisdiction is "one of status, namely, whether the accused in court-martial proceedings is a person who can be regarded as falling within the term "land and naval forces."

In McElroy v. United States ex rel.. Guagliardo and Wilson W. Bohlender, 80 S. Ct. 305 the petitioners were civilian employees of the armed forces who were tried by court-martial for noncapital offenses. Both individuals were convicted and both appealed their convictions. They contended that the military did not have jurisdiction to try them for noncapital offenses committed overseas. The Supreme Court upheld the petitioners and ruled the military did not have jurisdiction to try a civilian who commits a noncapital offense overseas during peacetime.

The US Supreme Court, through its decisions in these cases, established the general rule that civilians offenders, who commit offenses while accompanying the armed forces overseas during peacetime, cannot be tried by military court-martial under Article 2(11) of the Code.

Wartime Jurisdiction. The jurisdiction over "persons serving with or accompanying an armed force in the field" in wartime is granted expressly by the UCMJ. The Supreme Court has never denied military jurisdiction over civilians accompanying the armed forces in the field during wartime. In his opinion in Reid v.Covert, Justice Black alludes to the exercise of military jurisdiction over civilians in time of war under Article 2(10) of the Code. In part, he said:

> "There have been a number of decisions in the lower federal courts which have upheld military trial of civilians performing services for the armed forces "in the field" during time of war. To the extent that these cases can be justified, insofar as they involved trial of persons who were not "members" of the armed forces, they must rest on the Government's war powers." In the fact of an actively hostile enemy, military commanders necessarily have broad power over persons on the battlefront. From a time prior to the adoption of the Constitution, the extraordinary

> circumstances in an area of actual fighting have been considered sufficient to permit punishment of some civilians in that area by military courts under military rules."

In wartime, it is clear the military can exercise court-martial jurisdiction over civilians accompanying armed forces "in the field". In a number of cases, the exercise of such jurisdiction has been upheld.

In United States v. Averette, the accused was a civilian employee of an Army contractor in Vietnam. He was tried and convicted by general court-martial for conspiracy to commit larceny and attempted larceny. On review, the Court of Military Appeals held Averette was not subject to trial by court-martial.

In reaching the decision, the Court stated that the words "in time of war" mean, for the purposes of Article 2(10)...a war formally declared by Congress.

Because Congress had not formally declared war in Vietnam, the court held the accused was not subject to court-martial jurisdiction. In addition, the Court was careful to note it was not expressing--

> "An opinion on whether Congress may constitutionally provide for court-martial jurisdiction over civilians in time of a declared war when these civilians are accompanying the armed forces in the field. Our holding is limited--for a civilian to be triable by court-martial in 'time of war', Article 2(10) means a war formally declared by Congress."

Since Congress had not formally declared war in Vietnam, the military did not have jurisdiction to try Averette by court-martial for the offenses with which he was charged.

Conclusion. Decisions of the Supreme Court and the Court of Military Appeals have held peacetime court-martial jurisdiction over civilian dependents an employees in overseas situations is unconstitutional. Neither the Supreme Court nor the Court of Military Appeals has rule on the issue of whether civilian dependents and employees accompanying an armed force in a wartime are subject to court-martial jurisdiction. Other federal court, however, have upheld the exercise of military jurisdiction in such cases. The Court of Military Appeals, while not passing on the constitutionality of wartime jurisdiction, has strictly construed the term "time of war" to mean a time when war has been declared formally by Congress.

LESSON 1

PRACTICE EXERCISE 1A

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. What is the definition of jurisdiction?

2. What document defines United States military jurisdiction?

3. Service members are the only category of people subject to military court-martial jurisdiction for noncapital offenses in time of peace.

   ○ A. True.

   B. False.

4. Recently, the Supreme Court extended the military's criminal court jurisdiction over military members.

   A. True.

   B. False.

5. What are the two Supreme Court decisions that have had a major impact on the court-martial jurisdiction of the military over its members? and .

PRACTICE EXERCISE 1A
ANSWER KEY AND FEEDBACK

1. What is the definition of jurisdiction?

   The right, power, or authority to administer justice.

2. What document defines United States military jurisdiction?

   The Constitution.

3. Service members are the only category of people subject to military court-martial jurisdiction for noncapital offenses in time of peace.

   A. True.

   B. False.

4. Recently, the Supreme Court extended the military's criminal court jurisdiction over military members.

   A. True.

   B. False.

5. What are the two Supreme Court decisions that have had a major impact on the court-martial jurisdiction of the military over its members? O'Callahan and Solorio.

PART B: CI INVESTIGATIONS WITHIN THE MILITARY JURISDICTION SYSTEM

In this part of Lesson 1, you will learn:

* The concept of investigative jurisdiction.
* The definition of apprehension.
* The provisions of the Delimitations Agreement.
* The conduct of investigations of national security crimes.
* The proper handling of different types of physical evidence.

INVESTIGATIVE JURISDICTION.

The jurisdiction of military counterintelligence (CI) investigative authority is set forth in AR 381-10, AR 381-20, and the Delimitations Agreement. The investigative jurisdiction of CI units and elements encompasses all matters within their mission, except as limited by regulations and agreements by Department of the Army with other agencies. In essence--

> "The Army will conduct aggressive, comprehensive, and coordinated counterintelligence activities world-wide, to defect, identify, assess, and counter, neutralize, or exploit the intelligence collection efforts, other intelligence activities, sabotage, subversion, sedition, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against Department of the Army (DA) or Department of Defense personnel, information, material, and activities. This mission will be accomplished during peacetime and all levels of conflict".

DELIMITATIONS AGREEMENT.

The Delimitations Agreement is a document that specifies both the investigative jurisdiction and limitations that apply to each military service and the Federal Bureau of Investigation (FBI). In implementing the personnel security program, it became necessary to conduct investigations on certain persons to determine their loyalty to the US. The Delimitations Agreement spells out the responsibilities and limits of the FBI and each service to prevent investigative agencies from interfering with each other. It also prevents duplication of effort by the four agencies (FBI, Army, Navy, and Air Force).

Purpose.

The agreement was established in 1949, by the Office of the Deputy Chief of Staff for Intelligence, US Army; Office of Naval Intelligence, US Navy; Office of Special Investigations, Inspector General, US Air Force; and the FBI. This agreement, commonly known as the "Delimitations Agreement," concerns the responsibilities of the signatories for the investigation of all activities coming under the categories of espionage, counterespionage, criminal subversion, and sabotage. This agreement is binding upon all US Army investigative agencies. Under the agreement, the responsibility assumed by each organization carries with it the obligation to exchange freely and directly all information of mutual interest. When the organization, with primary operating responsibility is unable for any reason to produce material in that field desired by the subscribing agencies, special arrangements are worked out through negotiation at the national level. These negotiations take place before activity by one agency in another agency's field. Close cooperation and coordination between the four subscribing organizations is a mutually recognized necessity.

NOTE: The Office of Naval Intelligence has been re-designated as the Naval Investigative Service.

Responsibilities.

Following is a list of the responsibilities set forth in the agreement to include appendices and supplemental agreements:

FBI.

All investigations of espionage, counterespionage, criminal subversion, and sabotage cases involving civilians and foreign nationals of all classes in the Continental US, Alaska, Hawaii, Puerto Rico, and the Virgin Islands.

All investigations of violations of the Atomic Energy Act of 1946. There are no territorial or personnel limitations on this provision.

The coordination of the investigative activities of civilian agencies in the US, Puerto Rico, and the Virgin Islands that provide information regarding subversive movements and activities in these categories.

Keeping the other subscribing organizations advised of important developments in espionage, counterespionage, criminal subversion, and sabotage within its cognizance, particularly--

* Activities of inactive reserves of the armed forces, including the National Guard.

* Developments affection plants engaged in armed forces contracts.

* Developments concerning the strength, composition, and intention of subversive civilian groups within its cognizance whose activities are a potential danger to US security.

* Developments affecting those vital facilities and vital utilities designated by the Secretary of Defense.

* Developments affecting critical points of transportation and communication systems designated by the Secretary of Defense.

Military Services: The following agencies represent investigative authority for the respective military services:

The Office of the Deputy Chief of Staff for Intelligence, DA (DCSINT, DA); the Naval Investigative Service; and the Office of Special Investigations, Inspector General, US Air Force.

In general, these organizations are responsible for the following:

* The investigation and disposal of all cases of espionage, counterespionage, criminal subversion, and sabotage involving active and retired personnel of that particular service.

* The disposal, but not investigation, of all cases in these categories involving civilian employees of the particular service in the US, Puerto Rico, and the Virgin Islands.

* The investigation and disposal of all cases in these categories involving civilian employees of the particular service stationed in areas other than the US, Puerto Rico, or the Virgin Islands, except the part of the investigations that have ramifications in the US, Puerto Rico, or the Virgin Islands.

* The investigation of all cases in these categories involving civilians and foreign nationals who are not employees of the other subscribing organizations, in areas where the commander of the particular service has supreme jurisdiction over the armed forces stationed therein, including possessions of the US other than Puerto Rico and the Virgin Islands.

* Informing the other subscribing organizations of any important developments.

NOTE: The Navy and Air Force have special provisions involving a section of Alaska.

Where the above paragraphs involve general territorial coverage, responsibility for such coverage will pass from one element of the armed forces to another automatically with change of command

responsibility. This provision is subject to modification by direct agreement between the interested elements of the armed forces.

While investigative jurisdiction of the civilian populace in former enemy territories occupied by the armed forces has been provided for above, those provisions are subject to direct adjustment with the State Department, if and when that department assumes governmental direction in such area of occupation.

From time to time, it may be desirable to modify or amend the Delimitations Agreement. Subject to the exceptions already provided for above, general amendments or modifications involving all of the four subscribing organizations will be issued in the form of a revised Delimitations Agreement and not as separate instructions.

During periods of martial law or periods of predominant armed forces interest not involving martial law, when agreed upon by the subscribing agencies, the provisions of Appendix A or B to the Delimitations Agreement will also apply.

All agreements of a continuing nature and applicable to two or more of the subscribing agencies to the Delimitations Agreement that effect its effect its basic jurisdiction will be reduced to writing. Then they will become supplements to the Delimitations Agreement and distributed to the extent agreed upon by the co-signers.

Army Investigations Under AR 381-10.

Army CI investigations may target both non-US persons, if the criteria outlined in AR 381-10 are met. To determine if such a situation exists, the following analysis must be performed:

* Is the anticipated investigation within the CI mission as stated in AR 381-20?

* Who are the subjects? Are they US persons (US citizens, legal resident alien, US corporations, or, organizations composed mainly of US persons), or are they non-US persons? Are they active duty Army or are they civilians?

* Does the Army have the primary jurisdiction based on the Delimitations Agreement?

* If the Army does not have jurisdiction, what types of information may be collected? (See AR 381-10.)

* What collection methods may be used and what approvals must be secured before initiating? (See AR 381-10.)

* Once the information is acquired, may it be kept or disseminated? (See AR 381-10.)

In general, this analysis highlights key items as addressed in AR 381-10; namely that CI agents only become active where they are authorized to do so, that the constitutional rights of US persons are protected, and that intelligence collection is a vital mission in respect to our national defense that must be performed to the maximum extent possible consistent with the law.

APPREHENSION.

"Apprehension" is defined as the act of taking a person into custody based on a legal warrant or authority. The main point is that military intelligence (MI) investigations do not involve apprehension. However, it is necessary to know when CI agents can apprehend and who they can apprehension. However, it is necessary to know when CI agents can apprehend and who they can apprehend.

Pursuant to 10 USC 807-809, 28 USC 535, Rules for Court-martial (RCM) 302, AR 600-40, and this regulation, CI agents are authorized to apprehend any person subject to the UCMJ, regardless of location, if there is a reasonable belief that the person has committed a criminal offense under United States Army Intelligence Agency USAIA Investigative jurisdiction CI agents are also authorized to conduct investigative stops of any person subject to the UCMJ, regardless of location, if there is a reasonable suspicion that the person has committed a criminal offense under USAIA, investigative jurisdiction.

CI agents are authorized to detain civilian personnel on military installations or facilities when there is a reasonable belief that the person has committed a criminal offense against the U.S. Army, and the offense is within USAIA investigative jurisdiction. CI agents are also authorized to conduct investigative stops of civilians on military installations or facilities, if there is a reasonable suspicion that the person has committed a criminal offense under USAIA investigative jurisdiction. Civilian will be detained only until they can be released to the FBI.

Army CI agents may not apprehend or detain civilians outside the limits of a military installation or facility within the United States. When an apprehension is necessary in the conduct of a CI investigation, an arrest warrant must be obtained and executed by a civil law enforcement officer. CI agents may accompany the arresting official for the purpose of identifying the person to be arrested and to provide assistance as authorized in AR 500-51.

Apprehension of civilians off a military installation or facility outside the United States may be authorized if host nation authorities consent and the proper arrest warrant is obtained.

Personnel apprehended by CI agents will be released to civil or military police, as appropriate, for processing detention, or confinement.

NATIONAL SECURITY CRIMES.

US Army CI Agents are specially trained to detect and investigate espionage, sabotage, treason, sedition, criminal subversion, disaffection, and all others and then initiate action to prevent and neutralize the treat posed to US Army command, personnel, and functions by these activities. These activities are collectively termed "national security crimes."

Sabotage.

Definition. The essence of the crime of sabotage (Title 128, USC, Chapter 105, Sections 2151-2156) is the deliberate injury, destruction , or defective production of national defense or war materials by either an act of commission or omission.

It can be anticipated that acts of sabotage, both in overseas areas-of-operation and in the Continental US, will increase significantly in future wars, regardless of the type or level of conflict.

Sabotage is a particularly effective weapon of guerilla and partisan groups, operating against logistical and communication installations in occupied hostile areas, and of insurgents in internal defense operational areas. Acts of sabotage may be committed by trained saboteurs sponsored by hostile guerrilla, insurgent, or intelligence organizations. They may also be conducted by individuals operating independently and motivated by revenge, hate, spite, or greed. During limited war when guerrilla forces are active, internal defense measures must distinguish between acts involving clandestine enemy agents or dissatisfied friendly personnel from overt acts of war perpetrated by armed enemy units.

Types of Sabotage. Incidents of sabotage or suspected sabotage normally are classified according to the means employed. The traditional types of sabotage have been incendiary, explosive, and mechanical. In the future, chemical, biological, and nuclear means of sabotage may be used this will pose an even greater threat to military operations.

Investigative Procedure in Sabotage Investigations. Because the first indication of sabotage normally will be the discovery of the e injury, destruction, or defective production most sabotage investigations will be incident-type cases (that is, cases involving an unknown person or persons). Immediate action is of paramount importance in conducting a sabotage investigation. The saboteur may still be near the scene, or other military targets may require immediate additional security protection to preclude or limit further damage. Of vital significance is the preservation and analysis of the incident scene before the evidence is altered or destroyed.

Espionage.

The giving or selling national military or defense secrets to a foreign nation. Unlike sabotage cases, most espionage investigations will be personal subject rather than incident-type cases-that is, they will originate with allegations regarding the activities of know individuals. These are instances, however, when CI investigators will be directed to conduct investigations of incidents. In these cases, espionage is suspected, but the identity of suspects has not been established (for example, the theft of classified documents or material). Leads in espionage investigations may originate from a wide variety of sources, prominent among which are the following:

* Reports from confidential sources.

* Reports from other intelligence, security, and law enforcement agencies.

* Discovery of evidence of espionage during surveys, inspections, and technical surveys.

* Report submitted by military units in accordance with provisions of AR 381-12 regarding espionage directed against the US Army and its personnel.

* Discovery of evidence of espionage during screening of refugees, line-crossers, displaced persons, enemy prisoners of war, and similar groups.

* Information developed during the course of routine personnel security investigations.

* Information or evidence obtained through censorship operations.

Federal Espionage Statutes. The espionage statutes encompass many kinds of activities and have the ultimate goal of preventing defense information from falling into the hands of a foreign nation.

The salient aspects of the Federal Espionage Act, Title 18, USC, Sections 793-796, are summarized as follows:

Whoever, with the intent or reason to believe the information is to be used to the injury of the US or to the advantage of a foreign nation--

* Goes into a place connected with the national defense for the purpose of obtaining defense information;

* Copies anything connected with the national defense;

* With either lawful or unlawful possession, delivers national defense information to one not entitled to receive it, fails to deliver it on entitled to receive it; or,

* Receives or obtains any writing connected to the national defense with reason to believe it was obtained contrary to law will have committed a criminal violation of the espionage act.

In addition, anyone who attempts to communicate with the enemy during wartime; collects, communicates, or attempts to elicit information pertaining to the public defense; or with lawful possession, through gross negligence rather than intent, permits national defense information to be lost, stolen, or abstracted; or having knowledge of such loss, theft, or abstraction fails to make prompt report of the same will also have violated the act.

The punishment specified in the USC for most violations of the espionage act is a fine of not more than $10,000 or imprisonment for not more than 10 years or both. The exceptions are reproduced below from the USC:

18 USC 794(a)... Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit to any foreign government...or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly any information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

18 USC 794(b)...Whoever, in time of war, with the intent that the same shall be communicates, to enemy, collects records publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces...or war materials of the United States...or any other information relating to the public defense, which could be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

Espionage Under UCMJ.

The description of what constitutes espionage under Article 106a of the UCMJ is essentially the same as that under 18 USC section 794. The only significant difference found in the UCMJ is the potential punishment. For the following categories, a compromise of material could result in punishment by death for the accused:

* Nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation,

* War plans.

* Communication intelligence.

* Any other major weapon system or defense strategy.

NOTE: The death penalty pertains to both war and peacetime situations.

Spying. Although the crime of spying as defined in Article 106, UCMJ, differs from espionage, counterintelligence investigations (CIIs), based on Article 106, are to be categorized as espionage cases for reporting and statistical purposes. Spying is strictly limited to wartime military situation because of the requirements of international law, particularly the provisions of the Geneva Conventions. The four elements that constitute the crime of spying are as follow:

* Breach of our lines and apprehension within US zone-of-operations.

* Clandestine operations or false pretenses.

* Obtaining or seeking information to communicate to the enemy.

* Specific intent to so communicate.

NOTE: All four elements must be present to bring charges of spying.

Investigative Guidelines in Espionage Cases. Analysis of the statute and pertinent court decisions permit the following conclusions to the drawn with respect to proof of espionage:

"National defense information" is information of military significance which has not been published for public consumption; that is, not distributed in public channels. It need not be classified defense information as defined in AR 380-5. The critical points are it relates to the national defense and has been restricted to authorized channels.

"Any foreign nation" means the nation involved need not be a declared enemy, as in treason.

Loss through gross negligence requires no positive act because it is a crime of omission. Each facet (grossly negligent, loss, and failure to promptly report) is a separate and distinct crime.

The espionage investigation must be directed toward the collection of information to show whether:

* National defense information was involved.

* There was an intent or reason to believe the US would be injured, or a foreign nation would benefit.

* One or more of the acts enumerated in the statute actually occurred.

Conduct of Espionage Investigations. No single set of investigative procedures can be recommended as applicable to the conduct of espionage investigations. This is because of the wide variety of circumstances under which espionage cases may originate and the many different elements that may constitute the crime of espionage. In addition, it may not always be desirable to direct the course of the investigation toward the arrest and prosecution of the offender.

The following quotation from testimony in February 1950, by J. Edgar Hoover, then FBI Director, explains why arrest and prosecution are not always the objectives of espionage investigations:

> "In a criminal case, the identification and arrest of the wrongdoer are the ultimate objectives. In an espionage case, the identification of the wrongdoer is only the first step. What is more important is to ascertain his contacts, his objectives, his sources of information, and his methods of communications. Arrest and public disclosure are steps to be taken only as a matter of last resort. It is better to know who these people are and what they are doing, and to immobilize their efforts, than it is to expose them publicly and then go through the tireless efforts of identifying their successors."

Treason.

The abuse of treason statutes in English legal history led the framers of the US Constitution to include a limiting definition of reason in that document. The Constitution also imposes qualifications regarding the conviction of an individual for that crime. "...no person shall be convicted of treason unless on the testimony of two witnesses to the same overt act or on confession in open court." (Article III, US Constitution.)

CI investigations in which treason is alleged or suspected often occur during wartime. However, they are more apt to be opened immediately upon the conclusion of hostilities. Allegations of treason may originate with liberated prisoners of war, interned US civilians, examination of captured enemy records, or interrogation of enemy military and civilian personnel.

Elements of Treason Under Federal Statute. Interpretation by the federal courts in treason cases leads to the following generalities concerning the legal elements of the crime of treason under the federal statute:

The accused must owe allegiance to the US. A US citizen owes permanent allegiance whether in the US or on foreign soil, unless an effective renunciation of citizenship was made. An alien in the US owes temporary allegiance to the US because he enjoys the protection of US laws.

A levy of war must be an actual wage of open hostilities against the government with specific intent to cause its overthrow.

Aid and comfort to the enemy means, in general, any act committed after a state of war exists which indicates a want of loyalty to the US Government and sympathy with its enemies, and which by fair construction, is directly in furtherance of their hostile designs.

The levy of war and aid and comfort to the enemy are alternative acts, either of which, when done by a person owing allegiance to the US, constitutes treason.

The investigative burden in treason cases is as follows:

Allegiance to the US at the time of the act of treason must be shown.

A levy of war under the two following conditions must be shown:

* Open hostilities against the US Government.

* Specific intent to overthrow the US Government.

There must be an aid and comfort to the comfort to the enemy under these conditions:

* Tangible or intangible aid to an enemy must be shown.

* The enemy must be in a state of open hostility with the US Government.

Two witnesses to the same overt act must testify, or it must be established that the accused intends to confess in open court.

Aiding the Enemy. Investigations conducted by CI personnel to prove or disprove charges brought against a subject under Article 104, Appendices B and C, UCMJ, Aiding the Enemy, may in some cases be categorized as treason cases.

The article provides that "any person who (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things, or (2) without proper authority knowingly harbors or protects or gives intelligence to or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly shall suffer death or such other punishment as court-martial or other as a military commission may direct."

Physical Acts Which Constitute Aiding the Enemy. From the wording of the article and interpretation by the Court of Military Appeals, there are three physical acts that constitute the crime of aiding the enemy. Any on of these acts committed with general criminal intent is a violation of the article:

* Aiding the enemy with ammunition, arms, supplies, or other things.

* Harboring or protecting the enemy without proper authority.

* Giving intelligence to, communication with, corresponding with, or holding any intercourse with the enemy without proper authority.

Proof Requirements Under Article 104.

* It is necessary to prove only that one or more of the prohibited acts actually occurred.

* The enemy need not be a declared enemy but may be a "substantial" enemy. For example, communist forces in the Korean or Vietnam Conflicts.

* The requirements of proving allegiance and the overt act by two witnesses which are essential under the federal treason statute do not apply.

Korean Conflict Cases Under Article 104. Article 104 was used in the majority of the court-martial cases arising from the Korean prisoner of war incidents. Most of the specifications in these cases concerned that part of the act making correspondence without authority, a crime. The Court of Military Appeals established in these cases there are only three types of communication with the enemy that may be made with "proper authority" under military law:

* A communication disclosing name, rank, social security number, and date of birth.

* A communication concerning the necessities of life.

* A communication concerning regulations and orders of the place of confinement.

Conduct of Treason Investigations. Treason cases will almost always be personal-subject rather than incident cases. Unlike most other CIIs, the investigation of a treason case will be primarily concerned

with obtaining evidence of past rather than current activities. The CI Agent must give particular attention to the legal requirements governing the collection and preservation of evidence, especially the taking of statements from witnesses and suspects. He must be careful to sift fact from rumor or hearsay when taking testimony from witnesses and reporting the investigation results. In many cases, it will be necessary for the investigator to consult regularly with legal authorities during the course of the investigation to ensure the elements of proof are being fulfilled and all applicable legal conditions and restrictions are met.

Sedition.

CIIs regarding alleged or suspected sedition may be used on either the federal sedition statute (Sections 2384 and 2385, Title 18 USC) or the UCMJ (Article 94, Mutiny and Sedition). Leads or allegations that prompt the opening of sedition investigations by control offices may come from many sources. They are most often based on information submitted by confidential sources contained in reports from other agencies or developed during the course of routine background investigations (BI). CIIs involving sedition may occur with equal frequency in either peacetime or periods of hostilities.

Seditious Conspiracy. Section 2384 of Title 18, USC, make it a specific crime to conspire to overthrow the US Government. Unlike the general conspiracy statute, which makes it a crime to conspire to commit any federal crime, the seditious conspiracy statute does not require the commission of an overt act toward fulfillment of the conspiracy's objective. The crime of seditious conspiracy is complete when two or more persons have entered into agreement to overthrow the government, or to prevent, hinder, or delay the execution of any federal law. It should be noted seditious conspiracy is a conspiracy to actually overthrow, as distinct from a conspiracy to advocate overthrow. Advocacy of the Overthrow of the US Government. Section 2385 of Title 18, USC, also known as the Smith Act (see figure 1-1), enumerates four specific types of activity which, if done to cause the overthrow of the government by force or violence, constitutes sedition. The prohibited acts are:

* Advocating or teaching the duty or necessity of such overthrow.

* Printing, publishing, selling, or distributing written matter advocating or teaching the duty or necessity of such overthrow.

* Organizing a society or group whose purpose is to advocate or teach the duty or necessity of such overthrow.

* Being or becoming a member of a affiliated with such society or group knowing the purpose thereof.

Court decisions relative to advocacy of overthrow have established the advocacy must be calculated to incite persons to take imminent, lawless action toward the violent overthrow of the government. The mere advocacy or teaching of forcible overthrow of the government as an abstract principle, divorced from any effort to instigate action to that end, does not constitute the crime of sedition under the Smith Act. The requirement for the advocacy to "incite persons to take action" is of particular significance to the CI Agent. Considerable effort in any case alleging violation of the Smith Act will be directed toward proving the oral or written material involved intended to incite listeners or readers to take action.

THE SMITH ACT

Seditious Advocacy

* Advocacy of action.

* Systematically teach techniques to accomplish unlawful goals.

* Words must be used so as to incite imminent lawless action.

* A specific intent to overthrow the Government of the United States.

Seditious Membership

* Knowledge of any organization and its objective of over-throwing the Government of the United States by force or violence.

* Active membership furthering the objective of the organization.

* Specific intent to support the objective of the overthrow of the US Government by force or violence.

Figure 1-1. Components of the Smith Act

Mutiny and Sedition. CI personnel may be directed to investigate sedition or mutiny cases.

Such complaint-type cases may be either personal-subject or incident-type.

"Mutiny" is defined as collective effort to overthrow lawful military authority. It also includes, under Article 94, UCMJ, the creation of a riot or disturbance with the intent to overthrow lawful military authority. The offenses may be committed in two ways:

* By several persons acting in concert to refuse to obey orders from proper authority and with intent to override military authority.

* By a person, with a similar intent, acting either alone or in concert with others, creating violence or a disturbance. The investigation of incidents of mutiny normally will not be assigned to CI personnel unless the mutiny is believed to be related to hostile intelligence or subversive activities.

Article 94, UCMJ, makes it a crime for any person, with intent, to cause the overthrow or destruction of lawful civilian authority, or to crate in concert with any other person a revolt, or other disturbance against such authority.

Conduct of Sedition Complaint Investigation. Sedition cases may be either incident-type, as in the case of the discovery of literature advocating the violent overthrown of the US Government; or they may be personal-subject type, as in the distribution of such literature by known persons. Covert investigative techniques are likely to be applicable to the conduct of sedition investigations.

Subversive Activity and Disaffection.

The majority of CIIs conducted by CI personnel in most areas-of-operation will be in either the "subversive activity" or "disaffection" categories. Most of these will be personal-subject cases based on adverse loyalty information developed during routine Background investigation (BI); reports submitted by military units under AR 381-12; reports from other intelligence and security agencies; and leads obtained directly from sources used in CI special operations.

Neither subversive activity nor disaffection, as such, is defined as a specific crime in either the federal criminal code or the UCMJ. Subversion is a catch-all category of various illegal acts that seek to undermine lawful, legitimate government. The objective of such a CII, therefore, usually will be to determine if there is a need for some administrative action (for example, removal from the sensitive assignment to protect the security of the military command).

Subversive activity. "Subversive activity" is all other willful activities which do not fit the categories of sabotage, espionage, treason, or sedition, but which are intended to lend aid, comfort, or moral support to individuals, groups or organizations advocating the overthrow of the US Government by force or violence, or are otherwise intended to be detrimental to the national security of the US. This area is very vague since there are no statutory standards which must be met. The investigation must, however, fulfill the following:

* Determine what act occurred.

* Show the activity was detrimental to the national security, based on evidence of probative value.

* Show the activity did not rise to the level of treason, sedition, espionage, or sabotage.

Disaffection is a state of mind. Although the disaffected person may have criminal intent, there is no conduct involved. Hence, disaffection is noncriminal in nature. However, a person within the military establishment possessing disaffection creates a vulnerability in the national security.

Such a person is most susceptible to approach by persons whose objectives are inimical to the US. The CI Agent must show disaffection through such tangible indications such as oral statements, written statements in personal correspondence, and published material.

PHYSICAL EVIDENCE.

Physical evidence is tangible in nature and recognizable in form. It tends to prove or disprove a fact in dispute. It includes all articles and material collected in connection with an investigation to establish the identity of the perpetrator and the circumstances under which an incident occurred.

These articles and material are used to aid in the prosecution of the offender. However, the importance of physical evidence, which may be encountered in any type of CI operation, is not limited to those investigations likely to result in a court trial. Physical evidence is often the proper determination of administrative actions, such as the granting of a security clearance, the issuance of a visa for entry into the US, or the admission of an alien into the armed forces.

You are not expected to be an expert in physical evidence. The analysis of various items normally will require the services of one or more specialists, such as ballistics experts, chemist, and fingerprint technicians, to fully identify the item as contributing to or not contributing to the crime. However, as a CI Agent you should have a general knowledge of the value, limitations, and characteristics of physical evidence. You should also be able to recognize, collect, handle, and preserve evidence encountered during the course of investigation.

Documentary Evidence.

Documents are the most common items of physical evidence encountered by CI personnel.

Manuscripts, magnetic tapes, records, files, reports, sworn statements, photographs, video tape movies, pamphlets, maps, sketches, passports, identity papers, and documents are likely to be collected in CI operations.

Questioned Documents. Questioned documents are those whose validity is disputed. FM 19-20 describes various categories of questioned documents and types of assistance available from criminal investigation experts and laboratories. This assistance may be obtained through liaison with the appropriate Provost Marshal's Office.

Documents Containing Codes and Ciphers. Codes and ciphers (cryptography) are often used in communication between operational elements of espionage agencies. Unless the key to the system has been obtained, the investigator should not spend any time attempting to decrypt the message. The document, along with the history of the circumstances under which it was obtained and a brief summary of the related investigation, should be given to the nearest US Army intelligence and Security Command USAINSCOM or MI unit.

Documents Suspected of Containing Secret Writing. Secret writing or the concealment from visible detection of written material by means of invisible inks, specially treated papers, microphotography, and similar systems, are also important facets of espionage communication systems. Documents taken from espionage suspects, or otherwise obtained under conditions indicating the possible presence of secret writing, should be tested for indications of secret writing. FM 34-5(S/NOFORN) and DIAM 58-11(S) contain guidance on the handling of documents suspected of containing concealed writing. No attempt should be made to recover any secret text. The material should be forwarded through intelligence channels to a facility or agency where the expertise is available.

Other Types of Evidence.

Traces and clues often may be found in the form of latent fingerprints, firearms, and ammunition; indentations made by tools, tires, or shoes; and from deposits of foreign substances such as fibers, soil, and stains.

Fingerprints. Fingerprints offer one positive means of identifying individuals, since they never change throughout a person's lifetime. Surface fingerprints can be transferred, photographed, and developed by various techniques, thus providing invaluable evidence for purpose of identification. Detailed consideration of fingerprint patterns and methods of collection and preservation are included in FM 19-

20. Assistance from fingerprint experts can usually be obtained through liaison with the local Provost Marshal's Office.

Indentations and Fractures: Physical impressions and indentations left in various media are often of value as evidence. Examples are footprints, tool marks, and marking left on ammunition by the weapon from which it was fired.

Fibers. Hairs and fibers have distinctive characteristics which may be useful in identification.

They may be classified as animal, vegetable, mineral, and synthetic.

Soil and Stains. Samples of soil can provide information when examined microscopically and chemically. Studies may indicate a difference between soil and dust, the latter being composed chiefly of vegetable fibers.

Soil analysis may reveal the geological source of general origin, and at times specific areas of origin. Stains resulting from any cause are susceptible to analysis in a laboratory. They may be identified as food, vegetable matter, grease, oil, paint, rust, or body fluids.

Laundry Marks. Dry cleaning, laundry, and other clothing or linen marks, whether they are made with indelible or invisible ink, may provide valuable clues in identification. Police usually maintain records which can help with this type of identification.

Detective Dyes. Police at times use dyes and fluorescent powders that can be dusted or sprayed on items likely to be handled by suspects. Some of these are virtually indelible; others are invisible, but susceptible to detection under ultraviolet light for a prolonged period after contact.

Handling of Physical Evidence.

All CI Agents should be familiar with handling evidence or evidentiary property.

The CI Agent acquiring physical evidence is personally responsible for safekeeping until he turns it over to the designated custodian of unit evidence. The custodian is, thereafter, responsible for control and accounting of such items. Normally, an officer of the CI unit will be designated as custodian of evidence as an additional duty. For obvious reason, evidence must be securely stored and protected from the time it is acquired to the time of its use in legal or other proceedings. When applicable, sufficient quantities of evidentiary materials must be acquired to permit laboratory analysis and use in court. For physical evidence to be admissible in a court, it is often necessary to establish that the evidence was part of, and found at a particular place. For this reason, photographs should be taken of the scene showing the position of the evidence in relation to that scene.

Maintaining the chain of custody for evidence is important because it permits proof the piece collected at he scene is the same as that presented in court, was collected at the time specified, and was not tampered with or handled by unauthorized persons. The chain of custody for evidence is maintained by a Chain of Custody Document DA Form 3881. In addition to DA Form 19-31, classified items will also be covered by a security receipt. The use of DA Form 19-23, Military Police Property Identification Tag, provides a relatively easy method for identifying and inventorying property in custody.

For transmittal of classified evidence, three wrappers should be used as follows:

1. See FM 19-20 for more details on this subject.

Inner wrapper. The sealed container is wrapped and properly sealed. The following information should be placed on the wrapper: full address and return address of the transmitting agency; when appropriate, the notation "evidence--to be opened by laboratory personnel only," and the classification of contents. Except for the addresses, these notations are placed on all six sides of the package. An envelope containing two additional copies of the evidence receipts, two copies of security receipts, plus two copies of the letter of transmittal should be affixed to the inner wrapper.

Middle wrapper. The package is then wrapped and sealed a second time. The markings are the same as for the inner wrapper except no notation is made that the package contains evidence.

Outer wrapper. The package is then wrapped a third time and again sealed. The outer wrapper bears only the two addresses. However, a special handling notation must be made if the evidence is perishable, flammable, fragile, explosive, corrodible, or corrosive.

The letter of transmittal for shipment of evidence to a laboratory is prepared in accordance with instructions contained in FM 19-20 and the appropriate Program Management Guideline technical bulletin. Where appropriate, the following statements will be included in the letter of transmittal:

* Warning that the package contains evidence.

* Brief summary of the case.

* Brief history of the evidence.

* Specific list of items and their classification.

* Clear statement of request explaining reasons for transmittal of the evidence.

* Statement as to whether the evidence submitted has already been subject to examination.

* Special consideration or instructions.

Release of Evidence. Unclassified items of evidence will be released or disposed of in accordance with AR 190-22. In the case of classified items, AR 380-5, and other applicable regulations governing the handling or release of classified material will be used.

EVIDENCE RULES.

Definitions of proof, evidence and fact.

Proof: Anything which serves to convince one of the truth or falsity of a proposition.

Evidence: Anything that is legally presented before a court that clarifies the point in question.

Facts: A circumstance, event, or occurrence as it actually took place (the goal of proof and evidence).

Functions of the Judge, Jury, and Attorneys.

Judge: To decide questions of law and administer the rules of evidence.

Jury: Helps weight evidence and decide who is curable and to what degree.

Attorneys: To present the evidence to the judge and jury in the most persuasive manner of which they are capable.

Material, Relevant, and Competent. All evidence must be material, relevant, and competent to be admissible.

Material: The materiality of evidence is determined by its logical relation to an essential element of the case.

Relevant:

* Evidence will be relevant when it tends to prove or disprove a fact in issue. In this sense, its meaning is indistinguishable from materiality.

* Evidence may still be excluded, if it is too collateral or remote from the essential issue in the case.

Competent:

* A witness will be competent to testify if he is able to meet the following criteria: 1. To observe the incident. 2. Remember the incident. 3. Relate the incident. If he was intoxicated, currently insane, or considered an infant, he may be disqualified.

* Evidence must be competent in the sense it must be authentic, reliable, and trustworthy (for example, general hearsay is incompetent).

Real Evidence.

Any physical object can be considered as real evidence. Real evidence must meet the same requirements of materiality and relevancy that testimonial evidence must meet. In addition, the real evidence must be "authenticated" to be admissible.

Real evidence is authenticated when it is shown to be what it purports to be, and it is shown to be substantially unchanged from the state it was in when initially connected to the relevant facts.

Real evidence may be authenticated by proof of a complete chain of custody or by the testimony of a corroborating witness. Failure to establish a complete chain of custody is on of the biggest problems that affect MI investigations.

Witnesses.

In testimony, it is extremely difficult to distinguish between fact and opinion, for all of a witness' assertions could be said to be opinions. The law recognizes two separate classes of opinion testimony; lay and expert opinion.

Lay witness.

* A layman will be able to state his opinions on subjects of a generalized common knowledge such as colors, smell, tastes, height, size, and weight.

* A layman will be able to state his opinions and conclusions when he has personal knowledge of the facts and the average person could draw a conclusion from the facts.

* The witness will be required to state the factual basis for his opinion.

Expert witness.

* A court will accept the opinion of an expert witness when the subject matter is such the average person would not be able to draw conclusions.

* There must be a body of experience or special knowledge a court will recognize as being sufficiently distinct so an individual could specialize in it.

* The expert witness may base his testimony on personal observation of the facts of a case presented to him in the form of a hypothetical question.

The jury may reject the opinions of either the lay or expert witness.

The judge will determine the admissibility of opinion testimony.

HEARSAY INFORMATION.

Hearsay is evidence about an out of court statement, that is being offered in court, as the truth. Normally, if this circumstance occurs, the evidence will not be allowed before the jury. To determine if the definition is met, the following analysis must occur:

* Out of court statement --The witness must be attempting to tell the judge and jury about a statement that the witness heard a third party make at another place and time.

* The truth of the statement--The testimony must be offered with the intent of having the judge and jury believe that the repeated statement was indeed made and was true. If the testimony is only offered to show that something was said, period, that testimony would not be hearsay.

* Exceptions--There are several exceptions to this rule, but the most important one, from CI point of view, is that if the out of court statement was a confession or admission, it would not be considered hearsay.

Procedures for taking testimony to be used as evidence.

Direct examination. The side which calls an individual as a witness may elicit information only by direct examination of that individual. The direct examination has the sole purpose of bringing out the facts within the personal knowledge of the witness, so far as that information is admissible under the rules of evidence. In general, the questions on direct examination cannot be leading; that is, they cannot suggest the form of the answer, assume a fact not testified to, or contain a conclusion of counsel.

Cross-Examination. After his direct examination, a witness may be cross-examined by the attorney for the opposing side. Cross-examination of a witness is a legal right and its denial is highly prejudicial to a criminal defendant. The purpose of the cross-examination is to place direct testimony in its true context to avoid misleading the fact-finding body. It is used to establish contradictions and improbabilities in the direct testimony in an effort to diminish or destroy the credibility of the witness. If a witness has indicated in a previously sworn statement that one fact exists and on the witness stand

tells a different story, the cross-examination attorney may point out the inconsistency during cross-examination. He attempts in that way to impeach the credibility of the witness.

The following are rules of privilege and prejudice:

Privilege. The law seeks to protect socially valuable relationships by protecting confidential communication that arises from them with an evidentiary privilege. Examples recognized in court include:

* Attorney--client privilege.

* Priest--pertinent privilege.

* Physician-patient privilege. (This relationship is not recognized in military practice, since no member of the Armed Forces may avoid medical treatment.) (For more information see DA Pam 27-22, Chapter 28.)

Governmental privilege.

* The privilege applies to information the government has that would be detrimental to the national interest if made available to the public.

* The privilege must be asserted by the head of the department that has the information, after he has personally considered the matter.

* If the judge determines the information is necessary to the accused's defense, if must be produced or the government must drop the prosecution.

Informer's privilege.

* The identity of government informants may be privileged if it is not necessary and relevant to the accused's defense.

* The contents of the informer's confidential communication may be privileged.

* If the person who made the communication is a government witness, then that report must be made available to the defense when it relates to the witness' testimony.

Prejudice.

* Some evidence that is material, relevant, competent, and not privileged may be excluded if allowing it would tend to prejudice the jury against the criminal defendant.

* The judge must balance the prejudicial effect of the evidence against its probative weight.

Circumstantial Evidence.

General. All evidence is divided into categories of "direct" and "circumstantial." Circumstantial evidence is any fact that gives rise to an inference as to the existence or nonexistence of a material fact in issue. It is not secondary or inferior to direct evidence; in many cases, it is the best evidence that can be obtained. Circumstantial evidence presents most of the problems concerning the relevance,

remoteness, and prejudicial effect of evidence. Direct evidence tends to prove or disprove a fact in issue.

The Inferential Process. Inferences are based upon unstated premises that are derived from the common experience of mankind. The more inferential steps that are required to establish the relevancy of some circumstantial evidence, the more progressively weaker the reasoning gets. It follows that we will have less confidence in the ultimate conclusion.

Character Evidence. Generally, character evidence will support a valid inference that the accused did or did not commit a specific criminal act. Evidence of a good or bad character by testimony is introduced by a competent witness as to the community reputation of the accused concerning his general character or a specific relevant character trait.

The prosecution is prohibited from introducing alleged specific acts of misconduct to prove the bad character of the accused. Unless the criminal defendant has placed his good character in issue, the prosecution may not introduce evidence of his bad character, because of the prejudicial effect this would have.

Past Criminal Record. Evidence of an accused person's past criminal record may be introduced to attack his credibility as a witness or to rebut evidence of good reputation when he puts his reputation in issue.

In addition, the criminal record may be proven to support a legitimate inference concerning the following material factors in a cases:

* Motive.
* Intent.
* Absence of mistake.
* Identity.
* Common scheme involving the commission of two or more closely related criminal acts.

The two inferences forbidden to be drawn from evidence of the accused's criminal record are:

* He as a bad character.
* He is predisposed to commit a crime.

LESSON 1

PRACTICE EXERCISE 1B

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. Military Intelligence investigative authority is set for .

2. The document which prevents duplication of effort by the FBI, Army, Navy, and Air Force is .

3. The US Constitution specifies that for a person to be convicted of treason, he must confess in open court or .

4. Anything which tends to prove or disprove a fact in dispute and is tangible in nature and recognizable is said to be .

5. To be admissible in court, all real evidence must be and .

6. Four of the national security crimes are , , and .

7. Under the Delimitations Agreement, which agency is responsible for investigations of violations of the Atomic Energy Act of 1946? .

8. MI CI Agents who are performing authorized CI investigations that disclose possible criminal activities are authorized to perform an apprehension.

   ○ A. True.

   B. False.

PRACTICE EXERCISE 1B
ANSWER KEY AND FEEDBACK

1. Military Intelligence investigative authority is set for AR 381-10, AR 381-20, and the Delimitations Agreement.

2. The document which prevents duplication of effort by the FBI, Army, Navy, and Air Force is The Delimitations Agreement.

3. The US Constitution specifies that for a person to be convicted of treason, he must confess in open court or there must be testimony of two witnesses to the same overt act.

4. Anything which tends to prove or disprove a fact in dispute and is tangible in nature and recognizable is said to be physical evidence.

5. To be admissible in court, all real evidence must be material, relevant, and competent.

6. Four of the national security crimes are espionage, sabotage, treason, and sedition.

7. Under the Delimitations Agreement, which agency is responsible for investigations of violations of the Atomic Energy Act of 1946? The FBI.

8. MI CI Agents who are performing authorized CI investigations that disclose possible criminal activities are authorized to perform an apprehension.

   A. True.

   B. False.

LESSON 2

DISLOYALTY, UNSUITABILITY, AND DEROGATORY INFORMATION

CRITICAL TASKS: **301-340-2001**

OVERVIEW

LESSON DESCRIPTION

In this lesson, you will learn how derogatory information provided to CI agents is used in loyalty/suitability investigations.

TERMINAL LEARNING OBJECTIVE:

TASKS: You will be able to list the types of activity that constitute disloyalty; identify individual characteristics that may cause someone to perform disloyal acts; and describe how derogatory information is handled.

CONDITIONS: You will be given narrative information and extracts from FM 34-60.

STANDARDS: Based on derogatory information received, you will conduct CI investigations into disloyalty and unsuitability in accordance with applicable regulations.

REFERENCES: The material contained in this lesson was derived from the following references in addition to the ones listed earlier in Lesson 1:

AR 635-200.
DA Pam 600-8.
FM 34-60.

INTRODUCTION

A CI investigation will usually concern an individual's loyalty and suitability for government service. An understanding of what constitutes disloyalty and unsuitability is essential for the proper conduct of these investigations.

This lesson has one part. At the end, there is a practice exercise. Answer all questions on the practice exercise and check your answers. Do NOT go on until you answer all the questions correctly.

PERSONNEL SECURITY PROGRAM.

Basic guidance for establishing a personnel security program is located in Executive Order 10450, which, in 1953, established the standards governing federal employment. EO 10450 states that an individual's acceptance or retention in federal employment must be clearly consistent with the national security. Under this standard, no true subversive could be found eligible for federal service.

EO 10450 also requires the disqualification from federal service on security grounds of all persons whose defective character, moral turpitude, questionable conduct, or other unfitness makes them subject to bribery, blackmail, or other pressure.

Definitions.

Personnel Security Investigations (PSI) serve as a basis for determining security acceptability for assignment and retention of military and civilian personnel in sensitive positions. Classified information or material will be entrusted only to persons cleared to receive such, and only when they have a need-to-know. The one type of PSI is the background investigation or BI.

Derogatory/adverse information is information that constitutes a possible basis for denial or revocation of security clearance or access to defense information. It may also be the basis for rejection or separation from service or employment with DA. In addition, it may be any information that would reflect unfavorably on an individual's loyalty, character, integrity, trustworthiness, and reliability. There are two categories: loyalty and suitability.

Adverse loyalty information is information that reflects unfavorably upon the loyalty of a US citizen.

Adverse suitability information is information that casts doubt upon an individual's character, trustworthiness, or reliability.

LOYALTY.

Rationale of the Loyalty Program.

The loyalty program exists to exclude true subversives from government employment. A true subversive is one who works to destroy our government by unlawful means. The government defends itself by setting a standard of conduct and then excluding true subversives from government employment because they do not meet that standard.

A loyalty action is not a criminal prosecution, but rather an administrative action to preclude security risks that would be caused by hiring subversives for government employment.

The acceptance or retention of any person in the military establishment must be clearly consistent with the interest of national security (EO 10450).

Specific criteria used to implement this standard in the Army are contained in AR 380-67.

Other binding regulations are:

* AR 600-37, which concerns unfavorable information.

* AR 604-10, which deals with the acceptance and retention of military personnel in the Army.

The logic of the regulation requires that when an individual's loyalty is in doubt, and his or her clearance is denied or revoked under, the individual must be processed for elimination under AR 604-10.

Rights of the Individual in Security Adjudications.

Civilians. The landmark case in this area, Greene v. McElroy, 360 US 474 (1959), showed that the constitution will not tolerate an arbitrary revocation of a security clearance. The Navy revoked Greene's security clearance and informed ERCO, Greene's employer, that the company would lose military contracts if Greene remained as an employee. Greene was fired by ERCO. He brought suit and won a decision in the Supreme Court. One of Greene's contentions was that he was denied the right to confront the witness against him.

DOD Civilian Employees. The Secretary of Defense was given the power to remove civilian employees without providing confrontation where national security would be seriously endangered. EO 10865 states if full confrontation is denied, the individual will be "given a summary of the information, which shall be as comprehensive and detailed as the national security permits." However, all cases to date have permitted full confrontation.

Military Members. Paragraph 6-7, AR 604-10 states the military member will "be confronted with the witnesses against him to the maximum extent possible...consistent with national security." While the military member receives less than a full confrontation at the hearing, the adjudicator will consider the fact that the military member "may have been handicapped in his defense by the nondisclosure to him of classified information or by the lack of opportunity to cross-examine persons constituting sources of such information."

Subversion Evidence.

Loyalty is Presumed. Disloyalty must be proved by evidence of subversive activity. The decision will be favorable to the subject if the agent fails to provide the adjudicator with evidence of subversive activity.

Grounds for finding a subject to be disloyal would include evidence that he has committed, attempted to commit, or conspired to commit any act of sabotage, treason, espionage, or sedition. All of these crimes contain an element of disloyalty. When a CI agent uncovers evidence of such crimes, his superiors will turn it over to the proper authorities for legal action.

Disloyalty can be proven only on the basis of an individual's actions not on his beliefs or reading habits. Consequently, the evidence used to prove disloyalty breaks down into the following categories:

* Evidence of active and knowing membership in a subversive organization.

* Evidence of subversive activity.

* Evidence of advocacy of the violent overthrow of the government.

Membership in a subversive organization - or even being a knowing but passive member of such an organization is not a sufficient basis for initiating a disloyalty investigation. The individual must not

only be aware of a subversive organization's unlawful goals, but also must be active in trying to achieve these unlawful goals.

Close, continuing association with a known subversive individual can be used as one criterion in gauging subversive activity. However, proof the individual sympathizes with the known subversive and acts with specific intent to aid the subversive in committing an unlawful act is required to begin a valid loyalty action.

The Smith Act establishes advocacy of the overthrow of the government by force or violence as a criminal offense. If an individual could be lawfully punished under the Smith Act, the individual may be legally rejected or eliminated from the military service on loyalty grounds.

Discharges. The usual approach for many years was to give an undesirable discharge to individuals removed from military service on loyalty grounds. This policy took into consideration the activities of an individual prior to, as well as during, military service. In the case of Harmon v. Bruker, 355 US 579 (1958), the Supreme Court held the Army could take into consideration the individual's record for his period of military service. Honorable service resulted in an honorable discharge.

SUITABILITY.

Definition of Adverse Suitability Information.

A character defect is defined as information which, although not reflecting adversely on an individual's loyalty to the US, does cast doubt upon his good character, integrity, trustworthiness, or reliability. It raises a doubt that granting him access to classified information is consistent with national security.

The Suitability/Security Connection.

Character defects do not necessarily mean a person is a security risk. However, past investigations of espionage directed against the US have shown that suitability is a matter of concern to agencies responsible for personnel security.

People whose character defects have made them vulnerable to blackmail may be referred to as pressure risks. If a subversive strikes at their weak points (character defects), they could become subversive risks, even though they are loyal to the US.

Suitability is not solely a security consideration. It is primarily a personnel matter. The personnel security clearance program's interest in suitability is limited to those areas in which there is a rational, demonstrable connection with security.

Suitability has an indirect relationship with security. It does not necessarily follow that persons who engage in conduct that abuses generally accepted standards of morality will act in a manner contrary to the best interest of national security. Many individuals who have served the military and the US Government faithfully have led less than virtuous personal lives.

Unsupported or unresolved unfavorable suitability information may severely prejudice an individual's reputation and future. Every instance of unsuitability does not necessarily indicate a security risk; this distinction must be understood by everyone concerned with the suitability phase of the personnel security program.

Suitability Action Adjudication.

The adjudicator cannot be arbitrary, unreasonable, or capricious he or she must avoid hasty decisions. Unless credible derogatory information concerning suitability is uncovered, an individual is presumed to be suitable and will be granted a security clearance.

A rational connection between a character defect and a security risk is needed to support any unfavorable decision. This rational connection demonstrates the security risk presented by an unsuitable person. Every person is a security risk to some degree. Absolute security may be achieved only by absolute immobility. The adjudicator's problem is to determine whether the risk is greater than the risk presented by the average person.

The danger to security from vulnerable or unreliable persons is apparent. An individual who fears exposure of something that he has done, or is doing, is a target for blackmail. An individual is unsuitable by virtue of his conduct in violation of personnel regulations or the UCMJ. The conduct creates the unsuitability and vulnerability because fear of exposure creates the security risk.

The ultimate determination must be an overly common sense determination based on all available information, both favorable and unfavorable. Consideration must be given to the gravity of the derogatory information, the age of the individual, and the circumstances existing when the incident occurred; subsequent conduct, behavior, and performance of duty. Isolated instances of youthful indiscretion must not be construed as permanent proof of a character defect.

SUMMARY OF THE BASIS FOR DENIAL OR REVOCATION OF CLEARANCE.

The ultimate determination of whether granting a clearance is clearly consistent with the interests of national security must derive from a common-sense interpretation of all available information, both favorable and unfavorable. The granting, denial, or revocation of a security clearance may be a matter of far-reaching consequences to DA as well as to the individual concerned. Therefore, arbitrary and perfunctionary decisions must be avoided.

Depending upon their seriousness, the activities and associations listed below, whether current or past, may be the basis for denial of access to classified defense information or revocation of clearance:

Commission of any act of sabotage, espionage, treason, sedition, or attempts, threat, or preparation thereof; or conspiring with or aiding or abetting another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

Establishing or continuing a sympathetic association with--

* A saboteur.

* A spy.

* A traitor.

* A seditionist.

* Anarchist or revolutionist.

* An espionage or secret agent.

* Representative of a foreign nation.

* Representative of a foreign nation whose interests are inimical to the interests of the US.

* Person who advocates the use of force or violence to overthrow the US Government or the alteration of the US Government by unconstitutional means.

Performing or attempting to perform his duties, to serve the interests of another government rather than the interests of the US.

Membership in, or affiliation or sympathetic association with, any foreign or domestic organization, association, movement, group, or combination of persons which is totalitarian, fascist, communist, or subversive. This includes organizations which have adopted a policy of advocating or approving the commission of acts of force or violence to deny other persons their rights under the US Constitution or which seeks to alter the form of the US Government by unconstitutional means.

Participation in the activities of an organization established as a front for an organization referred to above when the individual's personal views are sympathetic to the subversive purposes of such organizations.

Participation in the activities of an organization referred to above, in a capacity where the individual should reasonably have had knowledge of the subversive aims or purposes of the organization.

Participation in the activities of an organization with knowledge it has been infiltrated by members of subversive groups under circumstances indicating the individual was a part of, or sympathetic to, an infiltrating element or sympathetic to its purpose.

Sympathetic association with a member or members of an organization referred to above or sympathetic interests in totalitarian, fascist, communist, or similar subversive movements.

Currently maintaining a close continuing association with a person who has engaged in activities or associations of the type referred to above. A close continuing association may be considered to exist if the individual lives with, frequently visits, or frequently communicates with such person.

Close continuing association of the type described above, even though later separated by distance, if the circumstances indicate the renewal of the association is probable.

Any facts which furnish reason to believe the individual may be subject to coercion, influence, or pressure which may cause the individual to act contrary to the best interest of national security. Among matters which should be considered in this category are the presence of a spouse, parent, brother, sister, or offspring in a nation, a satellite thereof, or an occupied area thereof, whose interests are inimical to the interests of the US.

Failure or refusal to sign or pleading protection of the Fifth Amendment to the US Constitution or Article 31, UCMJ, in refusing to completely answer questions contained in Standard Form 86. Failing or refusing to answer any pertinent questions propounded in the course of an official investigation, interrogation, or examination, conducted for the purpose of ascertaining the existence or extent, or both, of conduct of the nature described above.

Willful violation or disregard of security regulations.

Intentional unauthorized disclosure to any person of classified information or disclosure of other information prohibited by any law.

Any deliberate misrepresentation, falsification, or omission of material fact.

Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct; habitual use of intoxicants to excess; drug abuse; or sexual perversion.

Acts of reckless, irresponsible, or wanton nature which indicate such poor judgment and instability as to suggest the individual might disclose security information to unauthorized persons or assist such persons, whether deliberately or inadvertently, in activities inimical to the security of the US.

All other behavior, activities, or associations which tend to show the person is not reliable or trustworthy.

Any illness, including any mental condition, of such nature which, in the opinion of competent medical authority, may cause significant defect in the judgment or reliability of the individual.

Any excessive indebtedness, recurring financial difficulties, unexplained affluence or repetitive absences without leave which would lead one to believe that the individual might act contrary to the best interest of national security.

Refusal to take the Oath of Allegiance or Oath of Service and Obedience.

Repeated acts of carelessness leading to inadvertent loss or compromise of classified material.

RELATIONSHIP BETWEEN SECURITY AND PERSONNEL REGULATIONS.

When a commander becomes aware of unfavorable information derived from intelligence files and security investigations, the commander will take one or more of the following actions:

* Suspend or deny access to classified information under the provisions of AR 380-67. Also, if necessary, initiate an investigation under the provision of AR 381-20 or other appropriate directives to ascertain the facts.

* Reassign the individual to a less sensitive position.

* Suspend favorable personnel actions (flag the soldier).

Access Suspension.

Commander's Options. A commander who becomes aware of credible derogatory information, falling within the scope of page E-1, AR 380-67, that concerns a member of the command who has a security clearance, will take one of the following courses of action:

Suspend the individual's access to classified information. Annotate DA Form 873, Part III. Conduct an inquiry or request an investigation from Defense Security Service (DSS), if appropriate. Complete DA Form 5248-R and forward to the US Central Personnel Security Clearance Facility (CCF) with DA Form 873 attached.

Suspend the individual's access and forward all derogatory information to the Commander, CCF, on DA Form 5248-R with commander's recommendation and DA Form 873 attached. Item II of DA Form

5248-R will indicate information forwarded is considered sufficient for determination and no further inquiry or investigation is pending or contemplated.

If the information available to the commander is insufficient to warrant suspension of access, or in a borderline case in which propriety of suspension action is questionable, forward the derogatory information to the CCF on DA Form 5248-R. This indicates access has not been suspended pending final determination by Commander, CCF.

If the individual is currently indoctrinated for Sensitive Compartmented Information (SCI) access, process suspension action in accordance with TB 380-35.

Reporting of Derogatory Information.

Initial Reports. Reports of access suspension will include a brief summary of the action that caused the suspension and will indicate that the commander or appropriate authorities are conducting an inquiry/investigation into the incident.

Follow-up Reports. Reports will be submitted at 60-day intervals if the commander has not taken final action, or for example if the matter is still pending action by civil court. A brief synopsis is all that CCF will require until the commander takes final action is taken by the commander.

Final Reports. At the termination of command action, a final report will be forwarded to CCF. The report will indicate the action taken as a result of the incident that caused the initial suspension. The final report should contain recommendations of the command concerning the subject's restoration of access or revocation action of the security clearance. It should include documentation of the derogatory information, for example, Military Police (MP) reports or blotter entries, AR 15-6 investigations, commander's inquiries, results of limited investigations, copies of courts-martial or Article 15s, medical reports or psychiatric examinations, and so on. CCF will not consider as final a report that subject is pending discharge under the provisions of AR 635-200. When the individual has been discharged, a copy of the discharge order will be forwarded to CCF as an enclosure to DA Form 5248-R.

Restoration of Access.

The Commander, CCF, is the only person designated to restore access suspended by a local commander. Restoration of access is accomplished by executing a new DA Form 873 with the information provided by CCF.

Elimination from Military Service Prior to Security Determination.

When revocation action is recommended and the individual is also being considered or processed for elimination from the US Army, the commander will monitor the individual's elimination action. He will take all appropriate measures to expedite the resolution of the proposed revocation before the subject elimination. If the individual is eliminated from military service before a final security determination by the Commander, CCF, the local commander will complete the following actions.

The Commander, CCF, will be notified the individual has been discharged. Notification will include full identifying data and refer to the report of access suspension. A copy of the order authorizing discharge will be forwarded as an enclosure to the DA Form 5248-R.

If the DA Form 873 was not previously forwarded to CCF, it will be withdrawn from the individual's Military Personnel Record Jacket (MPRJ) and the "Remarks" block annotated "Eliminated from the US Army for cause...(date)."

Denial/Revocation of Security Clearance.

Only the Commander, CCF, may deny or revoke a security clearance under the provisions of para 8-201(a), AR 380-67.

When credible derogatory information is received at CCF and an adverse security clearance action is contemplated, the Commander, CCF, will:

* Forward a letter of intent to deny or revoke a security clearance to the individual, through the commander.

* Provide a copy of the letter of intent to the appropriate office accredited by the US Army Investigative Records Repository (USAIRR).

* Forward the pertinent information for command action when the information available to CCF indicates disciplinary or elimination action may be warranted.

The commander will ensure the individual acknowledges receipt of the letter of intent by signing and dating the form letter enclosed with the letter of intent. The individual must indicate whether he intends to submit a rebuttal. The form letter acknowledging receipt of the Letter of Intent will be immediately forwarded to the Commander, CCF, by the official who presents the letter to the individual.

All replies to letters of intent will be endorsed by the individual's immediate commander and then sent through channels to the Commander, CCF. Endorsements should include commander's recommendation(s) relating to the individual's security clearance.

The additional time required to forward the individual's response through channels must be considered in the 60 days allowed for return of the letter of intent to CCF. Commanders will give the individual a realistic suspense date in which to reply to the letter of intent to allow adequate mailing time through channels.

If unusual circumstances will prevent the individual's reply from reaching CCF within 60 days a request for an extension must be furnished prior to the 60-day suspense. This letter must explain the reason for the delay and indicate the date by which CCF may expect the reply's arrival.

After receiving the response to the letter of intent, the commander, CCF will make a final determination and will then furnish it to the local commander. A copy will be furnished to the appropriate office accredited by the USAIRR.

A commander who receives a letter of intent to deny or revoke a security clearance concerning an individual who is no longer assigned to the unit, will take one of the following actions:

* If the individual was transferred, endorse the letter of intent and send it to the gaining command to complete the action. Forward an information copy of the endorsement to the Commander, CCF, ATTN: PCC-FP-RR.

* If the individual has separated/ discharged from the Army, advise the Commander, CCF, and furnish a copy of the separated/discharge orders.

When an individual is incarcerated by military or civil authorities following his conviction of a criminal offense, or when an individual is dropped from the rolls as a deserter, the commander will take the following actions:

* Withdraw the DA Form 873 from the individual's MPRJ and stamp, or print across the face, "Revoked by authority of the Commander, CCF, Deserter--(Date)," or "Revoked by authority of Commander, CCF, Incarcerated--(Date)."

* Forward the DA Form 873 to the Commander, CCF, ATTN: PCC-FP-RR, Fort George G. Meade, Maryland 20755.

Suspension of Favorable Personnel Actions.

Commanders and DA staff agencies must ensure favorable personnel actions are suspended for members against whom an investigation is initiated. Military or civilian authorities may initiate investigations into credible allegations or incidents that reflect unfavorably on the character or integrity of the member. The investigation begins when any of these authorities decides to investigate the involvement of the Army member.

Suspension will be initiated on all members, E-4 and above, when the investigation is formal. Suspension may also be initiated on any commissioned or warrant officer when an informal investigation could result in administrative, punitive, or disciplinary action.

Report suspension of favorable personnel actions on DA Form 268. (See Appendix D for a sample.) Commanders will prepare DA Form 268 or prepare a DA Form 4187 (Personnel Action) asking the Personnel and Administrative Center (PAC) to prepare the DA Form 268. The adjutant, executive officer, or deputy commander will sign DA Form 268. When DA staff agencies initiate a suspension, they will prepare DA Form 268 and distribute it. DA Form 268 prepared by a commander or PAC is sent to custodian of the MPRJ for distribution.

The commander will submit interim reports 2 months after the suspension action is initiated and every 2 months thereafter until the case is closed. (Example: a suspension initiated on 15 January 1995 will require an interim report to be submitted by 15 March 1997, until an interim report is no longer required or final report is submitted.) Exceptions are noted below:

Interim reports are required only once 15 May 1997, and so on, for a member dropped from the roll. Control of reports will be assumed by the command where the member is returned to military control for final disposition. An interim report is required upon the member's return to military control.

If the command has submitted an interim report stating that it has punished the subject by Article 15 or court-martial, no further interim reports are required.

For the above cases, the command will resume submissions when there is a change in status of the case or the member.

The commander will submit separate reports on each suspension action. For example, a member involved in an incident under investigation before the first suspense is closed, may become subject to another suspension action.

Reports on each suspension action are exempt from reports control under paragraph 7-2h, AR 335-15.

Distribution of interim and final reports will include the same distribution as the initial report.

The commander or DA agency that controls a suspension of favorable personnel action will ensure interim and final reports are submitted promptly. These reports are required to complete suspension control files. They protect the rights of its member. When interim or final reports are not received within a reasonable time by the addressee who received initial reports, the receiving command or agency will begin action to determine the status of the case.

Final unfavorable reports submitted on officers will include the following:

* Letters of reprimand, admonition, or censure to be included in the member's Official Military Personnel File (OMPF) (original and one copy). Letters will be processed according to Chapter 2, AR 680-37.

* Court-martial orders (two copies).

* All Article 15s.

The final DA Form 268 on enlisted members will include a summary of disciplinary or administrative action taken in block 18 (Synopsis of Available Information). Supporting documents are not needed.

For procedures on suspension of favorable action, see DA Pam 600-8.

Command Responsibility. In other than security cases, the responsible commander or DA agency initiating a suspension of favorable personnel action will maintain control until the case is closed or transferred to another commander.

In security cases, major commanders will establish procedures to submit and control suspension reports for all members for whom suspension action has been initiated under AR 604-10.

LESSON 2

PRACTICE EXERCISE

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. Information which casts doubt on an individual's character, trustworthiness, or reliability is .

2. When a commander becomes aware of credible derogatory information he must or .

3. The only person authorized to deny or revoke a security clearance under the provisions of paragraph 8-201 (a), AR 680-37 .

4. What three types of activity constitute disloyalty?

   .

5. An individual who is <u>not</u> disloyal but whose behavior makes him susceptible to blackmail or other inducements is said to be , which may make his access to classified information a risk to .

6. What did the Smith Act establish?

   .

7. When the issue is loyalty, policy requires that individual service members whose security clearances are revoked or denied must be .

8. When an individual's favorable personnel actions are suspended, interim reports are due from the initiating command every 2 months after the date suspension action is initiated until the case is closed. What are the two exceptions to this rule?

   A.

   B.

PRACTICE EXERCISE
ANSWER KEY AND FEEDBACK

1. Information which casts doubt on an individual's character, trustworthiness, or reliability is adverse suitability information.

2. When a commander becomes aware of credible derogatory information he must suspend his access and conduct an inquiry or request an investigation from DSS.

3. The only person authorized to deny or revoke a security clearance under the provisions of paragraph 8-201 (a), AR 680-37 is the Commander, CCF.

4. What three types of activity constitute disloyalty?

   Subversive activity. Active and knowing membership in a subversive organization. Advocacy of the violent overthrow of the government.

5. An individual who is not disloyal but whose behavior makes him susceptible to blackmail or other inducements is said to be vulnerable, which may make his access to classified information a risk to national security.

6. What did the Smith Act establish?

   The Smith Act established advocacy of the violent overthrow of the government as a criminal offense.

7. When the issue is loyalty, policy requires that individual service members whose security clearances are revoked or denied must be eliminated from military service.

8. When an individual's favorable personnel actions are suspended, interim reports are due from the initiating command every 2 months after the date suspension action is initiated until the case is closed. What are the two exceptions to this rule?

A. The member is dropped from the roll.

B. The member is undergoing punishment under UCMJ.

LESSON 3

RECORDING AND DISCLOSING INFORMATION

CRITICAL TASKS: **NONE**

OVERVIEW

LESSON DESCRIPTION

In this lesson, you will learn the legal restrictions on recording and disclosing information collected during a CI investigation.

TERMINAL LEARNING OBJECTIVE:

TASKS: You will be able to recognize valid requests for information under the Freedom of Information Act and the Privacy Act, distinguish between releasable and nonreleasable information under the provisions of those acts, and describe procedures for the collection, storage, and disclosure of personal information under the Privacy Act.

CONDITIONS: You will be given narrative information and extracts from AR 25-55 and AR 340-21.

STANDARDS: You will decide to release or retain information in accordance with the requirements of the Freedom of Information Act and the Privacy Act of 1974.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 25-55.
AR 340-21.

INTRODUCTION

The Freedom of Information Act and the Privacy Act of 1974 are related acts with a significant impact on the collection, storage, and disclosure of information. To be sure the record system under your supervision is being properly controlled, you will need to understand the provisions of these acts.

The lesson has two parts:

At the end of the lesson, there is a practice exercise. Answer all the questions on the practice exercise and check your answers. Do NOT go on until you answer all questions correctly.

PART A: FREEDOM OF INFORMATION ACT

In this part of Lesson 3, you will learn the following:

* The purpose of the Freedom of Information Act.
* The guidelines for release of information or denial of requests.
* The release and processing procedures for requests.
* The provisions of the act governing fee assessment and collection.

The US Army Regulation that implements the Freedom of Information Act (FOIA) is AR 25-55. Part 1 of Lesson 3 is derived primarily from this AR. If you are required to deal with requests for information under the Freedom of Information Act, consult AR 25-55 directly.

PURPOSE AND POLICY.

The public has a right to information concerning the activities of its government. It is Department of Defense (DOD) policy to conduct its activities openly and provide the public with a maximum amount of accurate and timely information about its activities.

AR 25-55 provides a formal control system designed to ensure compliance with FOIA. DOD personnel are expected to comply with the provisions of the FOIA in both letter and spirit. This strict adherence is necessary to provide uniform implement of the DOD FOIA program and uniformly and consistently to create conditions that will promote public trust.

A DOD record requested by a member of the public who follows rules established by proper authority in the DOD should be released. It may be withheld only when it is exempt from mandatory public disclosure under the FOIA. If a requested record is exempt under the FOIA, it may be released when it is determined no governmental interest will be jeopardized.

DEFINITIONS.

FOIA Discretionary Authority.

An exempted record must be made available upon the request of any individual when, in the judgment of the releasing DOD component or higher authority, its release would not jeopardize any government interest. DOD components should use their discretionary authority on a case-by-case basis in deciding whether to release given records.

This does not apply to exemptions 1, 3, or 6 listed below. It normally will not be exercised to release documents under exemption 4 unless that release will serve a compelling public interest.

Definition of Agency Record.

An agency record is any product of data compilation, regardless of physical form or characteristics, made or received by a DOD component in connection with the transaction of public business and preserved by a DOD component primarily as evidence of the organization, policies, functions, decisions, or procedures of the DOD component.

The following are not included within the definition of the word "record":

* Library and museum material made, acquired, and preserved solely for reference or exhibition.

* Objects or articles, such as structures, furniture, paintings, sculpture, three-dimensional models, vehicles, and equipment, whatever their historical value, or value as evidence.

* Commercially exploitable resources, including, but not limited to, formulae, designs; drawings; maps and charts, map compilation manuscripts and map research materials, research data, computer programs, and technical data packages that were not created, and are not used, as primary sources of information about organizations, policies, functions, decisions, or procedures of a DOD component.

* Unaltered publications and processed documents, such as regulations, manuals, maps, charts, and related geophysical materials available to the public through an established distribution system, with or without charges.

* Anything not a tangible or documentary record, such as an individual's memory or oral communication.

* Personal notes of an individual if not made available to other persons in an agency and not filed with agency records.

* Information stored within a computer for which there is no existing computer program or printout.

A record must exist at the time of the request to be subject to FOIA and AR 25-55. It must also be in DOD possession and control. A DOD component has no obligation to create, compile, or obtain a record to satisfy an FOIA request.

RELEASE OF INFORMATION AND DENIAL OF REQUESTS.

The FOIA gives seven reasons for not complying with a request for a record:

* The request is transferred to another DOD component, or federal agency.

* The requestor withdraws the request.

* The information requested is not a record within the meaning of the FOIA and AR 25-55.

* A record has not been described with sufficient detail to enable the DOD component to locate it by conducting a reasonable search.

* The requestor has failed to comply with procedural requirements, including payment of fees, imposed by AR 25-55 or DOD components supplementing regulations.

* The DOD component determines, through knowledge of its files and reasonable search efforts, that it neither controls nor otherwise possesses the requested record. (A "no record" determination is a denial; and may be appealed.)

* The record is denied in accordance with procedures set forth in the FOIA and AR 25-55.

Denial Tests.

To deny the release of a requested record in the possession and control of a DOD component, the component determine that the denial meets both of the following tests:

* The record is included in one or more of the nine categories of records exempt from mandatory disclosures.

* The use of the components discretionary authority to release the record is unwarranted.

Use of Exemptions.

Records that may be exempt shall be made available to the public when it is determined no government interest will be jeopardized by their release. Determination of jeopardy to governmental interest is within the sole discretion of the component, consistent with statutory requirements or other requirements of law.

Parts of the requested record may be exempt from disclosure under the FOIA. The proper DA official may delete exempt information and release the rest of the record to the person requesting it. If the nonexempt part of the record is unusable or does not contain a reasonable amount of information responding to the request, the DA official need not release it. Under FOIA, the proper official also has the discretion to release exempt information; but must exercise this discretion in a reasonable manner, within regulations.

FOIA Exemptions.

The following types of records may be withheld, in whole or in part, from public disclosure unless their release is otherwise prescribed by law.

Number 1. Records that were properly classified in the interest of national defense or foreign policy.

Number 2. Records containing or constituting rules, regulations, orders, manuals, directives, and instructions relating to the internal personnel rules or practices of a DOD component. These records may be withheld if their release to the public would substantially hinder the effective performance of a significant DOD function and they do not impose requirements directly on the general public.

Number 3. Records concerning matters that a statute specifically exempts from disclosure in terms that allow the command no discretion on the issue.

Number 4. Records containing trade secrets or commercial or financial information that a DOD component receives from a person or organization outside the government with the understanding that the component will retain the information on a confidential basis. Records within the exemption must

contain trade secrets or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information, impair the government's ability to obtain necessary information in the future, or impair some other legitimate government interest.

Number 5. Internal advice, recommendations, and subjective evaluations (as opposed to facts) pertaining to the decision-making process of an agency.

Number 6. Information in personnel and medical files, as well as similar personal information in other files, that, if disclosed to the requester, would result in a clearly unwarranted invasion of personal privacy.

This exemption shall not be exercised in an attempt to protect the privacy of a deceased person, but it may be used to protect the privacy of the deceased person's family.

If a requestor's interest can be adequately served by release of information not linked to a specific person, an Initial Denial Authority (IDA) may provide such information after deleting the names, personal identities, and other identifying information of persons other than the requestor.

As Individual's personnel, medical, or similar file may be withheld from him or his designated legal representative only to the extent consistent with the Privacy Act of 1974.

Number 7. Investigative records compiled to assist enforcement of civil, criminal, or military law, including the implementation of executive orders or regulations issued pursuant to law. IG investigative reports fall within this exemption.

This exemption however, applies only to the extent that release of a record or portion of a record would--

* Interfere with law enforcement proceedings.

* Deprive a person of the right to a fair trial or to an impartial adjudication.

* Constitute an unwarranted invasion of personal privacy of a living person, including surviving members of a deceased individual identified in such a record.

* Disclose the identity of a confidential source.

* Disclose confidential information furnished by a confidential source and obtained by a criminal law enforcement authority in a criminal investigation or by an agency conducting a lawful national security intelligence investigation.

* Disclose investigative techniques and procedures not already in the public domain and requiring protection against public disclosure to ensure their continued effectiveness.

* Endanger the life, or physical safety, of any individual.

This exemption does not diminish the right of individual litigants to investigative records currently available by law.

When the subject of an investigative record is the requestor of the record, it may be withheld only as authorized by the Privacy Act.

Number 8. Records contained in or related to examination, operation, or condition reports prepared by, on behalf of, or for the use of any agency responsible for the regulation or supervision of financial institutions.

Number 9. Records containing geological and geophysical information and data (including maps) concerning wells.

OPERATIONS SECURITY CONSIDERATIONS.

Release of information under the FOIA can have an adverse impact on operations security (OPSEC). The Army implementing directive for OPSEC is AR 530-1. That AR requires OPSEC points of contact be named for all Headquarters, Department of the Army (HQDA) staff agencies and all commands down to battalion level. Persons named OPSEC points of contact will be OPSEC/FOIA advisors.

DA Form 4948-R, Freedom of Information Act (FOIA)/OPSEC Desk Top Guide, (see Appendix E), lists references and information frequently used for FOIA requests related to OPSEC. The name and telephone number of the command OPSEC/FOIA advisor will be entered on the form. Persons who routinely deal with the public by telephone or letter on such requests should keep the form on their desks as a guide.

The command OPSEC/FOIA advisor should implement the policies and procedures describes in AR 530-1, consistent with AR 25-55. The remainder of this lesson will address proper procedures for handling all components of the FOIA.

TREATMENT OF CLASSIFIED DOCUMENTS.

Documents, or parts of documents that have been properly classified in the interest of national security must be protected. Classified documents may be released in response to an FOIA request only under Chapter 3 of AR 380-5. If an entire document cannot be declassified, the parts that require continued protection must be clearly identified. Any remaining parts that can reasonably be segregated may be released under AR 380-5.

The release of unclassified documents could violate national security. If this appears to be the case, FOIA personnel should request a classification evaluation under paragraphs 2-204, 2-600, 2-800, and 2-801 of AR 380-5. In such cases, other FOIA exemptions may also apply.

A combination of unclassified documents, or parts of them, could combine information that together might violate national security if released. If this appears to be the case, consider classifying the combined information per paragraph 2-11 of AR 380-5.

If a document or information is not properly or currently classified when an FOIA request for it is received, the request may not be denied on the grounds that the document or information is classified, except with the approval of the Army General Counsel.

OPSEC/FOIA advisors will:

* Advise persons processing FOIA requests on OPSEC requirements related to requests for documents.

* Help FOIA personnel prepare requests for classification evaluation.

* Help FOIA personnel identify the parts of documents that must remain classified under AR 25-55 and AR 380-5.

* Prepare a narrative description of those FOIA requests received during the reporting period that have OPSEC implications.

FOIA personnel and proponents processing FOIA requests must protect classified or exempted information; OPSEC/FOIA advisors do not relieve them of that responsibility.

RELEASE AND PROCESSING PROCEDURES.

Requests from Private Citizens.

The provisions of the FOIA are reserved for persons with private interests as opposed to governments seeking information. Foreign governments seeking information from DOD components should use established official channels to obtain information. Release of records to individuals under the FOIA is considered a public release of information.

Description of Requested Record.

Identification of the record desired is the responsibility of the member of the public who requests the record. The requester must provide a description of the desired record that will enable the government to locate the record with a reasonable amount of effort. The act does not authorize "fishing expeditions."

When a DOD component receives a request that does not "reasonably describe" the requested record, it will notify the requester of the defect. When practical, components will offer assistance to the requestor in identifying the records sought and reformulating the request to reduce the burden on the agency in complying with the Act. DA FOIA officials will reply to unclear requests by letter. The letter will address the following:

* Describe the defects in the request.

* Identify the additional types of information needed and ask the requester for such information.

* Tell the requestor no action will be taken on the request until the requestor responds to the letter.

* FOIA personnel may use the following guidelines, based on the principle of reasonable efforts, to deal with "fishing expedition" requests. Descriptive information about a record may be divided into two broad categories:

* Category I information is file-related. It includes information such as type of record (for example, memorandum), title, index citation, subject area, date the record was created, and originator.

* Category II information is event-related. It includes the circumstances that resulted in the record being created or the date and circumstances surrounding the event the record covers.

Generally, a record is not reasonably described if the description does not contain sufficient Category I information to permit FOIA personnel to conduct an organized, non-random search based on the component's filing arrangements and existing retrieval systems. This will be the case unless the request contains sufficient Category II information to permit implied Category I elements needed to conduct a search.

Ordinarily, when personal identifiers only are provided in connection with a request for records concerning the requestor, only records retrievable by personal identifiers will be searched. Such record searches may be conducted under Privacy Act procedures, but no record may be denied that is releasable under the FOIA.

The above guidelines notwithstanding, the decision of the DOD component concerning reasonableness of description must be based on knowledge of its files. If the description enables the DOD component personnel to locate the record with reasonable effort, the description is accurate.

Request Referrals.

Requests for records on loan to the DOD, which are restricted from further release and so marked, shall be referred to the agency that provided the record.

Public Domain.

Nonexempt records released under the authority of AR 25-55 are considered to be in the public domain. Exempt records released pursuant to AR 25-55 or other statutory or regulatory authority, however, may be considered to be in the public domain only when their release constitutes a waiver of the FOIA exemption. When the release does not constitute a waiver, such as when disclosure is made to a properly constituted advisory committee or to a congressional committee, the released records do not lose their exempt status. Also, while authority may exist to disclose records to individuals in their official capacities, the provisions of AR 25-55 apply if the same individuals seek the records in their private or personal capacities.

Authentication.

Records will be authenticated with an appropriate seal whenever necessary to fulfill an official government or other legal function. This service, however, is performed in addition to that required under FOIA and is not included in the FOIA fee schedule. DOD components may charge for the service at a rate of $3.00 per authentication.

FEES.

Fee Assessment.

Because agencies may not use fees to discourage FOIA requests, FOIA fees are limited to standard charges for direct document search and duplication. Documents may be furnished without charge or at a reduced charge when the agency determines that waiving or reducing the fees is in the public interest. Furnishing the information can be considered as primarily benefiting the general public. Based on this guidance, DOD has established a liberal fee schedule.

To be as responsible as possible to FOIA requests, while minimizing unwarranted costs to the taxpayers, DOD components must adhere to the procedures described in AR 25-55.

Fees Collection.

An agency or component need not collect charges and fees before rendering the service unless it expects the costs to exceed the fee waiver and the requestor has not indicated a willingness in writing to pay. It frequently will be more practical for an agency to collect charges and fees when it provides the service or property to the recipient if the requestor stated that the cost involved shall be acceptable or unacceptable up to a specified limit that covers anticipated costs. Advance collection of fees appropriate only when the requestor has not agreed in writing to pay the anticipated fee or has not honored previous commitments of paying fees owed an agency or component.

Duplication Fees

Type	Cost per Page
Printed Material	$ .01
Office Copy	$ .10
Microfilm	$ .25

Figure 3. FOIA Fee Schedule

PART B: PRIVACY ACT OF 1974

In this part of Lesson 3, you will learn:

* The purpose of the Privacy Act of 1974.
* The rights of individuals under the Act.
* The disclosure responsibilities of records custodians under the Act.
* The provisions of the Act or the collection and storage of information.
* The relationship of the Act to the FOIA and how that information is handled.

The Army Privacy Program, which implements the Privacy Act of 1974, is described in AR 340-21. Part 2 of Lesson 3 is derived primarily from this AR.

PURPOSE.

The Privacy Act of 1974 provides procedures whereby an individual may--

* Determine whether records pertaining to the individual exist within a specific system of records.

* Request access to such records.

* Request that record pertaining to the individual be amended because it is not accurate, relevant, timely, or complete.

It also protects individual privacy by limiting what, and under what conditions, the government agencies may lawfully collect and store personal information, and by limiting to whom personal records may be disclosed.

REQUEST PROCEDURES.

Requests to Determine the Existence of Records.

Upon providing written or oral request, an individual-or his or her authorized representative-will be informed whether a particular system of records contains any record pertaining to the individual. The requesting individual need only reasonably identify the system to be searched and provide any identifying information necessary to effect a proper search. Requests will be submitted to the official identified through the system notice. This official will answer requests within 10 working days of receipt and inform the individual how to request access to any record located. No fees will be charged for this search.

To assist the individual in determining if applicable records exist, Congress has required their publication in the Federal Register of Notices. This notice describes the various systems of records maintained by the Army.

It is imperative an individual seeking to exercise this right first consult these notices, discern those which may apply, and then reasonably identify the systems in any correspondence with the Army. This will ensure a prompt and accurate response from the Army. Individuals desiring assistance in identifying the system that may have records pertaining to them should contact Headquarters, Department of the Army (HQDA) (DAAG-AMR) Washington, DC 20314.

Requests for Access and the Freedom of Information Act.

When an individual or authorized representative requests disclosure of records, the Privacy Act applies only if those records--

* Pertain to the individual.

* Are contained in a system of records.

* Are retrieved through use of the individual's name and not some third party's identity.

Procedure for Requesting Access. An individual who desires access to any records within a system of records will take the following steps:

* Determine the existence of such records.

* If records are determined to exist, submit a written request as indicated in the applicable system notice. Such a request will reasonably identify the record within the system of records sought.

* If access is granted, pay any fee charged and provide any information or documentation requested.

* If access is denied, in whole or in part, the individual may appeal, if he so desires, to the Secretary of the Army, ATTN: Office of the General Counsel. Such an appeal will be addressed to the Access and Amendment Refusal Authority (AARA) for forwarding to the General Counsel.

* If the appeal is denied in whole or in part, the individual may seek judicial review of the denial.

Requests for Accounts of Certain Disclosures. Any individual or authorized representative may request information pertaining to disclosure of that individuals record(s) to others. Such requests shall be addressed to the records custodian.

Request for Amendment of Records.

Upon request, an individual or authorized representative may have a record pertaining to the individual amended by correction, addition, or deletion, if such record is not accurate, relevant, timely, or complete. The individual may do this is part of a system of records. Such requests will be processed in accordance with AR 340-21, of whether the Privacy Act is cited or not.

Procedures for Requesting Amendment of Records. An individual desiring amendment will--

* Submit a request to the records custodian, either orally or in writing. Request must contain sufficient information to permit the agency to identify and locate the records, a description of the item or portion for which amendment is requested, the reason(s) amendment the individual is requesting and if appropriate the documentary evidence supporting the requested amendment. The individual bears the burden of providing that the requested amendment's proper. The individual will also verification his/her identity, to ensure the individual is seeking amendment of only the individual's own records.

* Provide any additional information which may be required.

* If amendment is refused, in whole or in part, the individual may appeal if he or she so desires to the DA Privacy Review Board. The appeal will be addressed to the AARA who refused the amendment, for forwarding to the board.

If the appeal is denied, in whole or in part, the individual may--

* Submit, to the custodian of the record a concise statement setting forth the reasons for disagreement with the refusal of the board to amend.

* Seek, judicial review of the denial in accordance with Section 3(g) of the Privacy Act.

Reasons for Amendment. Requests for amendment in accordance with this regulation may be sought only when the record is alleged to be inaccurate as a determination of fact (rather than judgment), irrelevant, untimely, or incomplete. AR 340-21 does not permit the alteration of evidence presented in the course of judicial, quasi-judicial, or quasi-legislative proceedings.

Requests for amendment of judgmental matters must be processed under applicable existing procedures (for example, AR 623-105 for officer evaluation report appeals).

Exempt Reports. US Army Criminal Investigation Command (USACIDC) reports of investigation are exempt from amendment provisions of the Privacy Act.

PROCESSING REQUESTS.

Processing Requests for Access.

The official who receives a request will acknowledge receipt within 10 working days. Requests for access to records considered to be the property of another agency (within the meaning of the Privacy Act) or office within the DOD, or which are on loan to the using office (for example, investigative records) will be referred to the appropriate agency or office. Requests for other records contained in a system of records must be processed in accordance with this regulation and, if applicable, in coordination with the originating organization.

With respect to any portion of the record to which this official determines that access must or can be granted, the official will, within 30 working days of receipt, inform the individual of the following:

The individual may obtain access to the record either by mail, through copy reproduction or in person through personal inspection. Personal inspection will normally be allowed during duty hours at a location reasonably convenient to the requestor.

The agency may change only those costs of reproducing those copies desired by the individual. These charges will be at the rate specified in AR 25-55 and may be waived as provided therein, or otherwise within the discretion of the releasing official.

If the records would not be available to any member of the public under the Freedom of Information Act, the individual must provide reasonable verification of his identity.

* When access is requested in person, verification will normally be limited to information on documents which an individual is likely to have readily available (for example, driver's license, or an employee or military identification card). When an individual can provide no suitable documentation provided, a signed statement from the individual asserting his identity and indicating knowledge of the penalty for obtaining or requesting records under false pretenses (a fine of up to $5000) will suffice.

* When access is requested through the mail, the individual may have to provide certain minimum identifying data, such as name and date of birth.

If the sensitivity of the information contained in the requested record warrants, a signed and notarized statement similar to that described above, may be required.

NOTE: An individual cannot be denied access to a record solely because the individual refuses to provide a social security number, unless the number was required for access by statute or regulation adopted before 1 January 1975. An individual who requests access in person may be accompanied by another individual of that individual's own choosing, if so desired. The appropriate commander may require the individual to furnish a written statement authorizing any discussion of the records in the presence of the accompanying person.

As soon as the above administrative requirements are met, the releasing official will grant access to the records as requested. Any such record will be presented in a form comprehensible to the individual.

The releasing official determines access to any portion of the record must be denied, he will, within 10 working days of receipt of the request, do the following:

* Forward a copy of the request, together with a copy of the record involved and reason(s) for recommending denial, to the appropriate AARA.

* Notify the individual of this refusal.

With respect to any portion of the record to which the AARA decides to grant access, the individual will follow the procedures specified above. With respect to those portions which are denied to the individual, the releasing official will, within the same 30 day working period, take the following steps:

* Inform the individual in writing of reason(s) for doing so. This statement will include nondisclosure exemptions covered by the Privacy and Freedom of Information Acts, and the significant and legitimate governmental purpose served by nondisclosure.

* Advise the individual of his right to appeal through the AARA to the Secretary of the Army, Attention: Office of the General Counsel.

* Submit copies of the request, and individual's denial to the Office of the General Counsel.

An AARA who receives a notice of appeal will forward it to the General Counsel within 5 working days of receipt. This referral will include copies of all records requested by the individual, clearly indicating those portions to which access was denied, together with a detailed justification for the denial.

The Office of the General Counsel, on behalf of the Secretary of the Army and within 25 working days after receipt of the appeal letter, will decide on any appeal submitted.

Access Denial.

An individual may be denied access to a record if it was compiled in reasonable anticipation of a civil action or proceeding, or for any of the following reasons:

* It has been properly exempted from the disclosure provisions of the Privacy Act.

* It would not otherwise be required to be disclosed under the Freedom of Information Act (AR 25-55).

* There exists a significant and legitimate governmental purpose for doing so.

An individual will not be denied access to his or her record solely because it is exempt from disclosure under AR 25-55 (FOIA) or because its physical presence is not readily available. Access will not depend upon any requirement that the individual state a reason or otherwise justify a need for access.

If a record contains both releasable and exempt information, the releasable portions will be extracted and made available. For example, to protect the personal privacy of other persons who may be identified in a record, copy will be made, deleting only that information pertaining to those other individuals.

Processing of Requests for Amendment of Records.

The custodian of a record who initially receives a request for amendment will do the following:

Within 10 working days after receipt, acknowledge the receipt in writing. The acknowledgment will clearly identify the request and advise the individual when the individual may expect to be informed of action taken on the request. If the request is delivered in person, a written acknowledgment should be provided when the request is presented.

If the custodian needs further information to process the request, he should contact the individual immediately and explain the necessity of such information.

If the custodian determines amendment is proper because the record is inaccurate, irrelevant, untimely, or incomplete, he should make the necessary correction and advise the individual within 30 working days of the request.

If a disclosure accounting has been made, the custodian will advise all previous recipients of the record of the substance of the correction. The custodian will tell them they should give notice of this correction to everyone to whom they have disclosed the record.

Amendments of records will be physically accomplished, as circumstances warrant, by adding supplementary information, or by annotating, altering, obliterating, deleting, or destroying of the record or a portion thereof. NOTE: Files maintenance and disposition instructions in the AR 25-400-2 do not apply to amendment of records created before congress enacted the Privacy Act.

If the AARA believes amendment would be improper because the system containing the record has been exempted or otherwise, the AARA will forward the request, along with the records involved and the custodian's recommendation to the appropriate AARA within 5 working days after receipt. The AARA will inform the individual of this referral he acknowledges receipt of the request. The AARA may request further information.

If the AARA determines amendment is proper even if the system containing the record is exempt from the amendment requirement the custodian will promptly see the amendment is made in accordance with rules mentioned above.

If the AARA determines amendment is not proper, within 5 working days the AARA will--

* Explain to the individual in writing the reason(s) for not amending the records.

* Advise the individual further review may be requested by the DA Privacy Review Board and any such request should be addressed to the AARA for forwarding to the board.

* Furnish copies of the letters of request and denial to the board and the commander possessing the records.

If the board decides not to amend the records, it will inform the individual in writing of the reason(s) for not amending the record. It will also advise the individual of the following:

The individuals right to file with the records custodian a concise statement of the disagreement with the board's decision.

Any such statement will be made available to anyone to whom the record is subsequently disclosed, together with a brief statement (if the Army deems it appropriate) summarizing its reasons for refusing to amend the record.

Prior recipients of the disputed record will be provided a copy of any statement of dispute to the extent an accounting of disclosures was maintained.

The individuals right to seek judicial review of the agency's refusal to amend a record provided for in Section 3(g)(1)(A) of the Privacy Act.

The board will not uphold a refusal to amend a record as requested unless this refusal is supported by the General Counsel.

Disagreement Statements.

When an individual files a statement disagreeing with the board's decision not to amend a record, the custodian will clearly annotate the record. It will be annotated in such a manner as to be apparent to anyone who may subsequently have access, use, or disclose it. The annotation itself should be integral to the record and specific to the portion in dispute. The annotation is required for automated systems of records as well.

Statements of dispute need not be maintained as an integral part of the records to which they pertain. They should, however, be filed in such a way they can be retrieved readily whenever

the disputed portion of the records is to be disclosed, If there is any question of whether the dispute pertains to information being disclosed, the statement of dispute should be included.

When information that is the subject of a statement of dispute is subsequently disclosed, the disclosing authority must note the information is disputed and provide a copy of the individual's statement.

The disclosing authority may include a brief summary of the board's reasons for not making a correction when disclosing disputed information. Summaries will be limited to the reasons the board stated to the individual. The summary will be treated as part of the individual's record for purposes of granting access. However, it will not be subject to the amendment procedures.

PRIVACY PROGRAM RECORD KEEPING.

Privacy Case Files.

Each element of the Army that is involved in processing privacy act requests will establish privacy case files. These case files will include requests from, and replies to, individuals on whether a system contains a record pertaining to them; requests for access and approvals, initial denials, and final review actions; requests for amendment and final review action; coordination actions and related papers. Privacy case files will be used solely--

* In processing the requests.

* As a source of precedents for formulating policies and procedures.

* For processing other similar requests.

Under no circumstances will privacy case files be disclosed for use in making any other determination about an individual. Maintenance and disposition of privacy case files will be in accordance with instructions contained in AR 25-400-2.

Disclosure Accounting.

For every records system created, the records custodian will keep an accurate accounting of the dates, natures, and purposes of all disclosures for each record. The custodian will also keep the name and address of the agency or person to whom such a disclosure was made and a cross-reference to the basis or justification for each disclosure. This will include any written documentation required for release of a record for statistical or law enforcement purpose. This provision also applies to disclosures made at the request of, or with the consent of, the individual.

In some instances as in the case of records in file folders a disclosure accounting record for each individual may be made a part of the folder. However, a records custodian need not make a notation on a single document of every disclosure of a particular record, if the required information can be reconstructed from an accounting system whenever--

* Requested by the individual,

* Necessary to inform previous recipients of amendments or dispute, or

* Necessary to provide an audit trail for subsequent review of Army compliance.

The disclosure accounting record will be retained for at least 5 years after the last disclosure or for the life of the record, whichever is longer. No record of disclosure of the contents of this form need be maintained.

DA Form 4410-R, Disclosure Accounting Record (Appendix D), is authorized and encouraged for use in recording required disclosure accounting information. The development and use of local forms to record disclosures from Automatic Data Processing (ADP) or other specialized systems of records is also authorized.

COLLECTION OF PERSONAL INFORMATION FROM INDIVIDUALS.

The following paragraphs describe certain restrictions on, and procedures for, the collection of information pertaining to individuals, to include social security numbers. They also set forth the responsibilities of Army officials in connection with these forms. Certain systems of records may be exempted.

Any personal information that will be contained in a records system (except statistical records) will be collected directly from the individual to the greatest extent possible.

The collection of information from third parties will be minimized to reduce the possibility of obtaining erroneous, outdated, irrelevant, or biased information. Exceptions to this policy are permitted under the following circumstances:

* When there is a need to ensure accuracy of information supplied by an individual through verification with a third party, such as verifying information for a security clearance.

* When the information can be obtained only from a third party (for example, a supervisor's assessment of an employee's performance in a previous job or assignment) or a criminal investigation.

* When obtaining the information from the individual would present exceptional difficulties or result in unreasonable cost.

Informing Individuals from whom Information is Requested.

Each individual who is asked to furnish personal information, whether or not it is to become a part of a records system, must be informed of the authority for requesting disclosure. The only authority which may be cited is:

* The statute or executive order which specifically authorizes collection of the particular personal information requested.

* The statute or executive order which authorizes the Army to perform a function, the discharging of which requires this information be collected.

The individual must also be informed of the following:

The principal purpose or purposes for which the information is to be used- for example, to evaluate suitability or issue benefit payments. Generally, the purposes will be directly related to, and necessary for, the purpose authorized by the statute or executive order.

The routine uses to be made of the information.

Whether furnishing the information is mandatory or voluntary. For example, individuals must be informed whether the Army is required or authorized to impose any penalties on him for failing to respond.

The effects on the individual, if any, of not providing all or any part of the information. For example, the collecting agency could inform this in that all information requested is necessary to identify the individual properly an individual and evaluate his claim for benefits and that, without such information,

no benefits can be awarded. An individual should suffer no adverse effect for failing to provide information which is not in fact relevant and necessary. (An example of such a statement is shown in Appendix F.)

Notification is not required when an individual is asked to supply no more than the information which normally may be released without an unwarranted invasion of privacy, and when such information is currently and properly maintained in a records system. The notification requirement applies only when information is collected directly from the individual for example, when the individual personally completes a form, or when the individual discloses information to an official during an interview. A notification statement is not required for forms, reports, or formats which are completed from information previously compiled on the individual.

The notice to the individual may be made on the form used to collect the information or on a separate form. In either case, the statement will be furnished to the individual for retention if requested. This notification must be given regardless of the media used in requesting information. This is the case whether it is a "form" in the usual sense (for example, a preprinted document with a control number and an edition date) or a questionnaire, survey sheet, magazine response sheet, or report rendered on a blank sheet. When information is being collected in an interview, the interviewer must provide the individual interviewed with the notice in a form suitable for his retention.

SSN Disclosure.

Any Army official who asks an individual to disclose his SSN will tell that individual whether disclosure is mandatory or voluntary. The Army official will also inform the individual of the statutory or other authority (including regulations) that specifically allows or requires the Army to solicit a number and what uses the Army will be made of it.

When the SSN is the only personal information requested from an individual, EO 9397 and the applicable statute, AR, or other command or agency directive will be cited as authority for collecting the SSN. Where appropriate, notification to the individual for disclosure only of the SSN may be accomplished by a sign or poster which bears the required information, placed conspicuously in the area. If such sign is used, Army elements nevertheless should be prepared to furnish a copy of the statement to the individual on request.

Are request for disclosure of any personal information is requested in addition to the SSN, falls under previously stated provisions for notification.

An individual may not be denied any right, benefit, or privilege provided by law for refusing to disclose his or her SSN unless disclosure is required by federal statute, or unless it will be made to an Army element maintaining a records system that was in existence and operating before 1 January 1975. It is also the case unless disclosure was required under statute, AR, or other directive adopted prior to 1 January 1975.

The DA is not precluded from requesting disclosure of an SSN under circumstances other than described above. The individual however must be advised that disclosure of the SSN is voluntary. If the individual refuses to disclose the SSN, Army elements must be prepared to identify the individual by alternate means.

Upon entering into military service or civilian employment with the DOD, the individual will disclose his or her SSN. The SSN is the individual's service or employment identification number. The Army needs it to establish personnel, financial, medical, and other official records. The required notice will be provided the individual upon entrance. It will not be required whenever an individual is subsequently requested to give or verify SSN, provided--

* The SSN is requested solely for identification purposes in connection with official DOD or Office of Personnel Management records.

* No use will be made of this number outside of the DOD or Office of Personnel Management, except as provided by the Privacy Act.

Forms in Use Before 27 September 1975.

Forms in use before 27 September 1975, which are to be used after that date, must meet the notice requirements by use of a separate statement.

This statement must accompany each form subject to the provisions of the Privacy Act of 1974. This statement will be prepared on DA Form 4368-R (Data Required by the Privacy Act of 1974) (Appendix G).

For forms in a regularly-issued, numbered series, the DA Form 4368-R identification will be deleted. Also, the Privacy Act Statement will be assigned the same number as the form to which it pertains. For example, in the case of SF Form 86 (Questionnaire for National Security Position, the applicable notice will be designed "SF Form 86 - Privacy Act Statement."

Similarly for unnumbered, questionnaires, survey sheets, and reports which collect personal information and identify individuals, the DA Form 4368-R identification will be deleted. The Privacy Act Statement will be assigned the reports control symbol or Office of Management and Budget (OMB) approval number that authorizes collection of the information.

All Privacy Act Statements will be submitted with DA Form 1167 (Request for Approval of Form) and a prescribing directive to the head of the agency of the commander, ATTN: Forms Management Officer. The forms management officer will review statements for compliance with forms design principles.

Forms Initiated or Revised After 27 September 1975.

As forms are revised or new forms are issued, the Privacy Act Statement will be incorporated, if practical, in the body of each form, questionnaire, survey sheet, or report. When feasible, the Privacy Act Statement will be positioned before the information requested from the individual. When it is impractical to obtain the statement on the basic form, it may be printed on the reverse side of the form or a separate statement will be prepared. DA Form 4368-R will be used when a separate Privacy Act Statement is necessary. All statements will be reviewed and approved by appropriate privacy and forms management officials.

Other Agency Forms.

Forms originated by other agencies that the Army uses to collect personal information from individuals for entry into a system of records must contain a Privacy Act Statement. Use of any agency forms subject to the Privacy Act without a notification statement will be suspended immediately and the matter referred to the appropriate Army forms management official. The forms management official, through technical channels, will determine whether use of the form is local, command wide, or Army wide. Based on the outcome of this determination, the forms management official will refer the matter to the appropriate privacy official. The privacy official, in coordination with the principal Army user, will ensure preparation of a Privacy Statement for the form or take action to discontinue its use.

PRIVACY ACT OF 1974, AND FREEDOM OF INFORMATION ACT.

As you read in Part 1, the Freedom of Information Act concerns the rights of the public to obtain access to records maintained by agencies of the federal government. In implementing the Act, AR 25-55 provides procedures for gaining access to these records, guidelines for determining what records must be released, what must be denied, and specifications for the fees that may be charged.

The FOIA and Privacy Act of 1974 overlap and support each other in some ways. For instance, the fees that may be charged for records released under the Privacy Act are those specified in the FOIA. More importantly, the Privacy Act provides one major limitation on the FOIA. Except under certain circumstances, an individual or agency will not be granted access to their own personnel records or the personal records of another individual.

The provisions of the two acts for determining the release of information are not identical, so it is important to know which Act properly governs a request for information from records. If a request seems to be covered by both Acts, the governing Act will be the Privacy Act of 1974, even if the request was submitted under the FOIA.

However, a Privacy Act request for access to records should also be processed as an FOIA request. If any part of the requested material is to be denied, it must be considered under the substantive provisions of both the Privacy Act and the Freedom of Information Act. Any withdrawing of information must be justified under an exemption in each act.

LESSON 3

PRACTICE EXERCISE

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. Which regulation has a formal control system designed to ensure compliance with FOIA?

   .

2. If a member of the news media requests a nonexempt record that contains identifying information on another individual, can the record be released? If yes, how? If no, why not?

3. When exercising its discretionary authority, DOD components can release exempt records if the release does not jeopardize government interests.

   ○ A. True.

   B. False.

4. If an unclassified document should have been classified when an FOIA request is received but was <u>not</u>, can it be denied on the grounds it is classified?

   A. Yes.

   B. No.

5. Are personal notes made by an agent, but not communicated or made part of a file, subject to FOIA?

   A. Yes.

   B. No.

6. What action is taken by the DOD component if a request is received that does not "reasonably describe" the requested record?

7. The Army privacy program, which implements the Privacy Act of 1974, is found in which Army Regulation?

.

8. What is the purpose of DA Form 4368-R?

9. If an individual requests access to his own personnel record under FOIA and the request is denied, the provisions of what act should be used to justify the denial?

.

PRACTICE EXERCISE
ANSWER KEY AND FEEDBACK

1. Which regulation has a formal control system designed to ensure compliance with FOIA?

   AR 25-55.

2. If a member of the news media requests a nonexempt record that contains identifying information on another individual, can the record be released? If yes, how? If no, why not?

   Yes, by removing all identifying information from the record. This is the simple answer. The details of each case should be studied before a determination is made.

3. When exercising its discretionary authority, DOD components can release exempt records if the release does not jeopardize government interests.

   A. True.

   B. False.

4. If an unclassified document should have been classified when an FOIA request is received but was not, can it be denied on the grounds it is classified?

   A. Yes.

   B. No.

5. Are personal notes made by an agent, but not communicated or made part of a file, subject to FOIA?

   A. Yes.

   B. No.

6. What action is taken by the DOD component if a request is received that does not "reasonably describe" the requested record?

   DA FOIA officials will reply to unclear requests by letter. The letter will (1) describe the defects in the request, (2) explain the types of information needed and ask for such information, and (3) tell the requestor no action will be taken on the request until a response is received.

7. The Army privacy program, which implements the Privacy Act of 1974, is found in which Army Regulation?

   AR 340-21.

8. What is the purpose of DA Form 4368-R?

   DA Form 4368-R is a standard form for the Privacy Act Statement described. It is used with personal information collection forms when a separate Privacy Act Statement is necessary.

9. If an individual requests access to his own personnel record under FOIA and the request is denied, the provisions of what act should be used to justify the denial?

   Both FOIA and the Privacy Act.

LESSON 4

CI INVESTIGATIVE RESPONSIBILITIES AND LIMITATIONS

CRITICAL TASKS:	**301-340-2010**
	301-340-2011
	301-340-2012
	301-340-2013

OVERVIEW

LESSON DESCRIPTION

In this lesson, you will learn the precise legal restrictions imposed upon intelligence collection assets by EO 12333 and AR 381-10.

TERMINAL LEARNING OBJECTIVE:

TASKS: You will be able to describe collection, storage, and dissemination of information on US persons as provided by AR 381-10; describe the provisions of AR 381-10 for assignments of CI personnel; and describe procedures for reporting and investigating violations of AR 381-10.

CONDITIONS: You will be given narrative information and illustrations from AR 381-10 and AR 381-12.

STANDARDS: You will perform intelligence collection operations in accordance with the restrictions and prohibitions specified in EO 12333 and AR 381-10 and AR 381-12.

REFERENCES: In addition to previously listed references, the following additional materials have provided subject information for this lesson:

AR 335-15.
AR 381-10.
AR 381-12.

INTRODUCTION

The responsibilities and limitations of US Army CI investigations are specified in several documents which you should be familiar with. Some of the more important provisions of these documents are discussed in this lesson.

This lesson has two parts:

Part A: Information Collection.

Part B: Employee Responsibilities and Oversight.

At the end of each part, there is a practice exercise. Answer all the questions on the practice exercise and check your answers. Do NOT go on until you answer all the questions correctly.

PART A: INFORMATION COLLECTION

In this part of Lesson 4, you will learn:

* The definitions of "US persons" and "collection."

* The provisions of AR 381-10 regarding the collection of information to include when it may be done, who may be targeted, what methods may be employed and who the approving authority is, and what responsibilities individual collectors have.

The purpose of AR 381-10 is to outline procedures enabling DOD intelligence components to carry out their mission effectively while ensuring that the constitutional and privacy rights of US persons are protected. It does not authorize the collection of any information relating to a person or organization solely because of lawful advocate of measures opposed to government policy. This regulation is intended to complement other regulatory policies. It does not establish authority to carry out any activity but rather to serve as a guide for completion of missions designated by other regulations such as AR 381-12 or AR 381-20.

If there is ever a question of interpretation when applying this regulation, the supporting judge advocate should be the point of contact locally. If the problem cannot be resolved at that level, it should be referred, through command channels, to the DA General Counsel.

DEFINITIONS.

Before beginning a discussion of collection, it is necessary to ensure an understanding of basic terms that play an integral part in the collection process.

US Person.

A US citizen, an alien lawfully admitted for a permanent residence, an unincorporated association composed mainly of US persons or a corporation incorporated in the US unless it is controlled by a foreign government.

Collection.

Information shall be considered to be "collected" only when it has been received for use of an employee of a DOD intelligence component in the course of his official duties. Essentially what this means is: a DOD employee must receive the information and take some positive step such as putting it in a file or on a computer in order for it to be "collected." Therefore, if a cooperating source provided an agent with information and the agent did not record it and place it in any retrievable file, it has not been collected. If an intelligence component is unsure as to the collectability of information they have

received, they have the opportunity to send that information to higher headquarters for a determination. If this is done, there is a 90 day temporary retention period during which the information in question is not considered to be "collected." Upon receipt of an answer from higher headquarters, that information is either disposed of or it becomes collected.

COLLECTION.

Targets.

Intelligence components may target both US and non-US persons subject to several limitations:

No one may be targeted unless it is necessary to the conduct of a mission assigned to the collecting components.

The techniques being employed have had the approval of the necessary authorities.

When collecting on a US person, you are limited to the following categories of information:

* Information obtained through consent.

* Information that is available to the general public.

* Foreign intelligence which includes individuals involved in international terrorism and international narcotics activities.

* Counterintelligence.

* Information concerning sources for either their protection or to determine their credibility.

* Information derived from a lawful intercept of personal communications, to include information on family members if it is relevant to the scope of the investigation.

* Information concerning a person who is a likely target of terrorism.

* Information collected by overhead reconnaissance as long as it is not directed at one person.

Administration information.

When targeting a US person concerning foreign intelligence in the US, it must be done in an overt manner unless: 1) the intelligence is significant, 2) the intelligence can not be reasonably obtained by overt means, 3) coordination has been made with the FBI and 4) the proper approvals have been obtained.

General Guidelines.

The general guideline rule for performing collection is: Pick the least intrusive method possible, get the proper approval, and then collect. The least intrusive method would be to use publicly available information. The next step would be the use of cooperating sources, the third step would be the use of a technique that did not require Attorney General or judicial approval, and the last step would be to utilize a technique that does require Attorney General or judicial approval.

Specific Techniques.

What follows is a short synopsis of procedures 5-13 of AR 381-10. For a more detailed explanation or specific guidance, AR 381-10 or United States Army Intelligence and Security Command (USAINSCOM) DA Pam 27-1 should be consulted.

Electronic Surveillance. Unconsented surveillance may be conducted in the US with approval of the Foreign Intelligence Surveillance Act (FISA) court. This is obtained by sending a request through the appropriate command channels with the proper documentation establishing a probable cause to believe foreign intelligence is on-going. Unconsented surveillance outside the US can also be conducted with the proper approval (see AR 381-10) based on the same standard.

Consented surveillance, which constitutes one or more people in a group giving written consent to monitoring, may also be done inside and outside the US with the approval of the Secretary of the Army or his designee.

Concealed monitoring. This technique includes the use of electronic equipment, such as video cameras, which are designed to monitor activity other than conversations. If the individual has an "expectation of privacy," meaning that he can reasonably expect to be free from intrusion in certain areas, you must get approval under the provision of monitoring through electronic surveillance.

If an individual does not have an "expectation of privacy," such as when a sign is posted, you seek approval based on concealed monitoring found in procedure 6 of AR 381-10.

Physical Search. Unconsented physical searches may be performed by MI CI Agents for intelligence purposes on a military installation. Prior to conducting the search, approval must be obtained from the commander empowered to grant search authority. This decision must be based on probable cause that foreign intelligence activity is present. Unconsented physical searches off military installations are the jurisdiction of the FBI or host countries and must be accomplished through liaison.

Consented searches, for intelligence purposes, may be performed with the acknowledged consent of the individual to be searched or upon approval of a military judge.

Mail Search. When mail is in US postal channels, first class mail may not be opened for intelligence purpose but all other classes may be searched if coordination is made with the proper postal authorities (see AR 381-10). Mail of any class cannot be opened without a judicial warrant, regardless of it's location. An examination of the outside covering of mail may be done on any class of mail with the proper coordination (see AR 381-10). Mail searches outside US postal channels may be conducted if done with proper justification and based on the standards set forth for unconsented physical search, as found in AR 381-10.

Physical Surveillance. This technique consists of a covert, systematic, targeting of an individual's movements or acquisition of non-public information by an individual not visibly present other than through covert means. An example would be electronic monitoring.

When this technique is necessary for the accomplishment of the mission, utilization may be made after proper approval is secured (see AR 381-10).

Undisclosed Participation.

An intelligence agent may not participate in an organization that constitutes a US person, on behalf of the intelligence community, unless they disclose their identity or get prior approval from proper authority (see AR 381-10). This does not restrict an individual from joining an organization for purely personal reasons, sitting in a public meeting, or accepting information from a cooperating source who is a member of an organization.

Assistance to Law Enforcement.

DOD intelligence components may cooperate with law enforcement for the purpose of:

* Investigating or preventing foreign intelligence gathering, international narcotics activities or international terrorist activities.

* Protecting DOD employees, information, property, or facilities.

* Preventing, detecting, or investigating violations of law.

This cooperation may include providing information, equipment, training, or personnel. The only restriction placed on these activities is that the military must be careful to not perform a strictly law enforcement function.

RETENTION.

As long as information is collected in a lawful manner, still serving the purpose for which it was collected, and necessary to the conduct of authorized functions of DA intelligence components or government agencies, it may be retained.

In order to determine if these criteria are met, a review made by competent legal advisors is necessary. If the review cannot be accomplished satisfactorily at the local level, the information may be retained temporarily, with higher headquarters consulted as mentioned previously.

DISSEMINATION.

Except when required by law, the only time that information concerning US persons may be released is under the following conditions:

* The information was properly collected.

* The recipient is reasonably believed to have a need to receive the information for the performance of a lawful government function.

* The recipient is a DOD employee, a law enforcement entity, an intelligence agency, a federal agency, or a foreign government with whom the US has an agreement.

SPECIFIC RESTRICTIONS.

Experimentation on human subjects will be done only if there is a vital foreign intelligence or CI purpose to be served. Additional restrictions are as follows:

* The informed consent of the subject must be obtained in writing.

* The experiment must conform to guidelines established by the Department of Health and Human Services, which safeguards the welfare of the subject.

Lesson 4

Practice Exercise A

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. Is a subsidiary of a US corporation, incorporated under the laws of Japan, considered a US person?

   ○ A. Yes

   B. No

2. A DOD employee asks official questions of a source but does not record the responses and put them in a file. Is the information "collected."

   A. Yes

   B. No

3. Suitability information may be collected on a US person who is a potential source of foreign intelligence.

   A. Yes

   B. No

4. Information concerning the political views of the Refuge Support Group of Greater Los Angeles (a group made up primarily of US citizens) may be collected.

   A. Yes

   B. No

5. Billy Soultpourt is the subject of a CI investigation. He telephones his mother in the next state once a week. Can his mother's name and address be collected? Can information about his mother's financial situation be collected?

    A. Yes/No

    B. Yes/Yes

    C. No/No

    D. No/Yes

6. Can information about MSG Tom Heard, who resides off-post, who cultivates marijuana in his greenhouse, and then sells it to neighbors, be collected by DA intelligence personnel?

    A. Yes

    B. No

7. Elvis Hotter tries to enter a DA facility with a briefcase. When he is told that before he can enter, his brief case must be searched, he decides to turn and leave. At this point, can the briefcase be searched without Hotter's consent?

    A. Yes

    B. No

8. Can first class mail found within US postal channels be searched for intelligence purposes with proper approval?

    A. Yes

    B. No

9. If requested, may information held by a DA intelligence component be provided to the FBI?

    A. Yes

    B. No

10. Saleh Faad, a member of a local Students for the Freedom of Palestine located in Sierra Vista, Arizona, comes to you to provide inside information on the group. Are you authorized to collect this information?

    A. Yes

    B. No

PART B: EMPLOYEE RESPONSIBILITIES AND OVERSIGHT

RESPONSIBILITIES.

All employees will conduct intelligence activities pursuant to, and in accordance with applicable directives, laws, executive orders, and regulations.

Familiarity.

Each DOD intelligence component shall familiarize its personnel with the provisions of AR 381-10, EO 12333, and any other law pertaining to their activities. At a minimum, everyone should be familiar with procedures 1-4 of AR 381-10, a summary of collection techniques and what their individual compliance and reporting requirements are.

Reporting.

Employees are required to report any violation of law, executive orders, or regulation, commonly called "questionable activity," that pertains to intelligence operations. This report will take the form of an electrical message routed through command channels to HQDA (DAMI-CIC), Washington, DC 20310 as soon as possible but no later than 5 days. The report should include:

* Description of the activity.
* Date, time, and location of occurrence.
* Person or unit responsible.
* Summary of incident.
* Status of investigation.

The initial investigation of the incident should be completed by the local command within 30 days and a report should be sent to HQDA containing the results and disciplining or corrective action taken.

OVERSIGHT.

The government has taken the position that increased intelligence gathering is essential to protecting our national defense. However, the constitutional rights of individuals must not be totally sacrificed to achieve this end. In order to ensure that a balance exists, oversight committees have been established to ensure that intelligence collection activities remain within the law.

The oversight committees consists of specifically designated organizations and people, who are tasked to periodically check intelligence components for compliance with appropriate laws and guidelines and then to report on their findings. In the Army, this responsibility has been delegated to the Inspector General, the General Counsel, and the Deputy Chief of Staff for Intelligence (DCSINT). Their job is to detect and prevent violations.

The purpose of the oversight personnel is to protect the integrity of the intelligence community as well as the rights of the people. Both of these missions are vital to ensure that we have the most professional

and skilled intelligence community possible that truly serves the country and people it is charged to protect. These people are to be worked with, not against.

LESSON 4

PRACTICE EXERCISE B

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, review that part of the lesson which contains the portion involved.

1. What is questionable activity?

2. How is questionable activity reported?

3. Who has oversight responsibility in the Army?

LESSON 4

PRACTICE EXERCISE B
ANSWER KEY AND FEEDBACK

1. What is questionable activity?

   Any violation of law, executive order, or regulations that pertains to intelligence activities.

2. How is questionable activity reported?

   By electrical message to HQDA as soon as possible but no later than 5 days.

3. Who has oversight responsibility in the Army?

   IG, General Counsel, DCSINT.

APPENDIX A

THE WHITE HOUSE

Office of the Press Secretary

For Release After **December 4, 1981**

EXECUTIVE ORDER 12333

UNITED STATES INTELLIGENCE ACTIVITIES

TABLE OF CONTENTS

UNITED STATES INTELLIGENCE ACTIVITIES

Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents is essential to the national security of the United

States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available. For that purpose, by virtue of the authority vested in me by the Constitution and statutes of the United States of America, including the National Security Act of 1947, as amended, and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART I GOALS, DIRECTION, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO THE NATIONAL INTELLIGENCE EFFORT

1.1 Goals. The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.

(b) All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.

(c) Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.

(d) To the greatest extent possible consistent with applicable United States law and this Order and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

1.2 The National Security Council.

(a) Purpose. The National Security Council (NSC) was established by the National Security Act of 1947, to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security. The NSC shall act as the highest Executive Branch entity that provides review of, guidance for, and direction to the conduct of all national foreign intelligence, counterintelligence, and special activities, and attendant policies and programs.

(b) Committees. The NSC shall establish such committees as may be necessary to carry out its functions and responsibilities under this Order. The NSC, or a committee established by it, shall consider and submit to the President a policy recommendation, including all dissents, on each special activity and shall review proposals for other sensitive intelligence operations.

1.3 National Foreign Intelligence Advisory Groups.

(a) Establishment and Duties. The Director of Central Intelligence shall establish such boards, councils, or groups as required for the purpose of obtaining advice from within the Intelligence Community concerning:

(1) Production, review, and coordination of national foreign intelligence;

(2) Priorities for the National Foreign Intelligence Program budget;

(3) Interagency exchanges of foreign intelligence information;

(4) Arrangements with foreign governments on intelligence matters;

(5) Protection of intelligence sources and methods;

(6) Activities of common concern; and

(7) Such other matters as may be referred by the Director of Central Intelligence.

(b) Membership. Advisory groups established pursuant to this section shall be chaired by the Director of Central Intelligence or his designated representative and shall consist of senior representatives from organizations within the Intelligence Community and from departments or agencies containing such organizations, as designated by the Director of Central Intelligence. Groups for consideration of substantive intelligence matters will include representatives of organizations involved in the collection, processing, and analysis of intelligence. A senior representative of the Secretary of Commerce, the Attorney General, the Assistant to the President for National Security Affairs, and the Office of the Secretary of Defense shall be invited to participate in a group which deals with other than substantive intelligence matters.

1.4 The Intelligence Community. The agencies within the Intelligence Community shall, in accordance with applicable United States law and with the other provisions of this Order, conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States, including:

(a) Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities;

(b) Production of dissemination of intelligence;

(c) Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, Organizations, persons, and their agents;

(d) Special activities;

(e) Administrative and support activities within the United States and abroad necessary for the performance of authorized activities; and

(f) Such other intelligence activities as the President may direct from time to time.

1.5 Director of Central Intelligence. In order to discharge the duties and responsibilities prescribed by law, Director of Central Intelligence shall be responsible directly to the President and the NSC and shall:

(a) Act as the primary advisor to the President and the NSC on national foreign intelligence and provide the President and other officials in the Executive Branch with national foreign intelligence;

(b) Develop such objectives and guidance for the Intelligence Community as will enhance capabilities for responding to expected future needs for national foreign intelligence;

(c) Promote the development and maintenance of service of common concern by designated intelligence organizations on behalf of the Intelligence Community;

(d) Ensure implementation of special activities;

(e) Formulate policies concerning foreign intelligence and counterintelligence arrangements with foreign governments, coordinate foreign intelligence and counterintelligence relationships between agencies of the Intelligence Community and the intelligence or internal security services of foreign governments, and establish procedures governing the conduct of liaison by any department or agency with such services on narcotics activities.

(f) Participate in the development of procedures approved by the Attorney General governing criminal narcotics intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(g) Ensure the establishment of the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products;

(h) Ensure that programs are developed which protect intelligence sources, methods, and analytical procedures;

(i) Establish uniform criteria for the determination of relative priorities for the transmission of critical national foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such intelligence;

(j) Establish appropriate staffs, committees, or other advisory groups to assist in the execution of the Director's responsibilities;

(k) Have full responsibility for production and dissemination of national foreign intelligence, and authority to levy analytic tasks of department intelligence production organizations, in consultation with those organizations, ensuring that appropriate mechanisms for competitive analysis are developed so that diverse points of view are considered fully and differences of judgment within the Intelligence Community are brought to the attention of national policymakers;

(l) Ensure the timely exploitation and dissemination of data gathered by national foreign intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government entities and military commands;

(m) Establish mechanisms which translate national foreign intelligence objectives and priorities approved by the NSC into specific guidance for the Intelligence Community, resolve conflicts in tasking priority, provide to departments and agencies having information collection capabilities that are not part of the National Foreign program advisory tasking concerning collection of national foreign intelligence, and provide for the development of plans and arrangements for transfer of required collection tasking authority to the Secretary of Defense when directed by the President;

(n) Develop, with the advice of the program managers and departments and agencies concerned, the consolidated National Foreign Intelligence Program budget, and present it to the President and the Congress;

(o) Review and approve all requests for reprogramming National Foreign Intelligence Programs funds, in accordance with guidelines established by the Office of Management and Budget;

(p) Monitor National Foreign Intelligence Program implementation, and, as necessary, conduct program and performance audits and evaluations;

(q) Together with the Secretary of Defense, ensure that there is no unnecessary overlap between National Foreign Intelligence Programs and Department of Defense Intelligence Programs consistent with the requirement to develop competitive analysis, and provide to and obtain from the Secretary of Defense all information necessary for this purpose;

(r) In accordance with law and relevant procedures approved by the Attorney General under this Order, give the heads of the departments and agencies access to all intelligence, developed by the CIA or the staff elements of the Director of Central Intelligence, relevant to the national intelligence needs of the departments and agencies; and

(s) Facilitate the use of national foreign intelligence products by Congress in a secure manner.

1.6 <u>Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies</u>.

(a) The heads of all Executive Branch departments and agencies shall, in accordance with law and relevant procedures approved by the Attorney General under this Order, give the Director of Central Intelligence access to all information relevant to the national intelligence needs of the United States, and shall give due consideration to requests from the Director of Central Intelligence for appropriate support for Intelligence Community activities.

(b) The heads of departments and agencies involved in the National Foreign Intelligence Program shall ensure timely development and submission to the Director of Central Intelligence by the program managers and heads of component activities of proposed national programs and budgets in the format designated by the Director of Central Intelligence, and shall also ensure that the Director of Central Intelligence is provided, in a timely and responsive manner, all information necessary to perform the Director's program and budget responsibilities.

(c) The heads of departments and agencies involved in the National Foreign Intelligence Program may appeal to the President decisions by the Director of Central Intelligence on budget or reprogramming matters of the National Foreign Intelligence Program.

1.7 Senior Officials of the Intelligence Community. The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, as appropriate, shall:

(a) Report to the Attorney General possible violations of federal criminal laws by employees and of specified federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department or agency concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(b) In any case involving serious or continuing breaches of security, recommend to the Attorney General that the case be referred to the FBI for further investigations;

(c) Furnish the Director of Central Intelligence and the NSC, in accordance with applicable law and procedures approved by the Attorney General under this Order, the information required for the performance of their respective duties;

(d) Report to the Intelligence Oversight Board, and keep the Director of Central Intelligence appropriately informed, concerning any intelligence activities of their organizations that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive;

(e) Protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the Director of Central Intelligence;

(f) Disseminate intelligence to cooperating foreign governments under arrangements established or agreed to by the Director of Central Intelligence;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of intelligence resulting from criminal narcotics intelligence activities abroad if their departments, agencies, or organizations have intelligence responsibilities for foreign or domestic narcotics production and trafficking;

(h) Instruct their employees to cooperate fully with the Intelligence Oversight Board; and

(i) Ensure that the Inspectors General and General Counsels for their organizations have access to any information necessary to perform their duties assigned by this Order.

1.8 The Central Intelligence Agency. All duties and responsibilities of the CIA shall be related to the intelligence functions set out below. As authorized by this Order; the National Security Act of 1947, as amended; the CIA Act of 1949, as amended; appropriate directives or other applicable law, the CIA shall:

(a) Collect, produce, and disseminate foreign intelligence and counter-intelligence, including information not otherwise obtainable. The collection of foreign intelligence or

counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(b) Collect, produce, and disseminate intelligence on foreign aspects of narcotics production and trafficking;

(c) Conduct counterintelligence activities outside the United States and, without assuming or performing any internal security functions, conduct counterintelligence activities within the United States in coordination with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(d) Coordinate counterintelligence activities and the collection of information not otherwise obtainable when conducted outside the United States by other departments and agencies;

(e) Conduct special activities approved by the President. No agency except the CIA (or the Armed Forces of the United States in time of war declared by Congress or during any period covered by a report from the President to the Congress under the War Powers Resolution (87 Stat. 855)) may conduct any special activity unless the President determines that another agency is more likely to achieve a particular objective;

(f) Conduct services of common concern for the Intelligence Community as directed by the NSC;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized functions;

(h) Protect the security of its installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the CIA as are necessary; and

(i) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) through (h) above, including procurement and essential cover and proprietary arrangements.

1.9 <u>The Department of State</u>. The Secretary of State shall:

(a) Overtly collect information relevant to United States foreign policy concerns;

(b) Produce and disseminate foreign intelligence relating to United States foreign policy as required for the execution of the secretary's responsibilities;

(c) Disseminate, as appropriate, reports received from United States diplomatic and consular posts;

(d) Transmit reporting requirements of the Intelligence Community to the Chiefs of United States Missions abroad; and

(e) Support Chiefs of Missions in discharging their statutory responsibilities for direction and coordination of mission activities.

1.10 The Department of the Treasury. The Secretary of the Treasury shall:

(a) Overtly collect foreign financial and monetary information; policy concerns;

(b) Participate with the Department of State in the overt collection of general foreign economic information;

(c) Produce and disseminate foreign intelligence relating to United States economic policy as required for the execution of the Secretary's responsibilities; and

(d) Conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President of the United States, the Executive Office of the President, and as authorized by the Secretary of the Treasury or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against such surveillance, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of the Treasury and the Attorney General.

1.11 The Department of Defense. The Secretary of Defense shall:

(a) Collect national foreign intelligence and be responsive to collection tasking by the Director of Central Intelligence;

(b) Collect, produce, and disseminate military and military-released foreign intelligence and counterintelligence as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill national, departmental, and tactical foreign intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components outside the United States in coordination with the CIA, and within the United States in coordination with the FBI pursuant to procedures agreed upon by the Secretary of Defense and the Attorney General;

(e) Conduct, as the executive agent of the United States Government, signals intelligence and communications security activities, except as otherwise directed by the NSC;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director of Central Intelligence, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain military intelligence relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international

organizations, and ensure that such relationships and programs are in accordance with policies formulated by the Director of Central Intelligence;

(j) Direct, operate, control, and provide fiscal management for the National Security Agency and for defense and military intelligence and national reconnaissance entities; and

(k) Conduct such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (a) through (j) above.

1.12 Intelligence Components Utilized by the Secretary of Defense. In carrying out the responsibilities assigned in section 1.11, the Secretary of Defense is authorized to utilize the following:

(a) Defense Intelligence Agency, whose responsibilities shall include:

(1) Collection, production, or, through tasking and coordination, provision of military and military-related intelligence for the Secretary of Defense, the Joint Chiefs of Staff, other Defense components, and, as necessary, non-Defense agencies;

(2) Collection and provision of military intelligence for national foreign intelligence and counterintelligence products;

(3) Coordination of all Department of Defense intelligence collection requirements;

(4) Management of the Defense Attaché system; and

(5) Provision of foreign intelligence and counterintelligence staff support as directed by the Joint Chiefs of Staff.

(b) National Security Agency, whose responsibilities shall include:

(1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense;

(2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

(3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;

(5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;

(6) Collection, processing, and dissemination of signals intelligence information for counterintelligence purposes;

(7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provision of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence;

(8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;

(9) Conduct of research and development to meet needs of the United States for signals intelligence and communications security;

(10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;

(11) Prescribing, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;

(12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and

(13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (11) above, including procurement.

(c) Office for the collection of specialized intelligence through reconnaissance programs, whose responsibilities shall include:

(1) Carrying out consolidated reconnaissance programs for specialized intelligence;

(2) Responding to tasking in accordance with procedures established by the Director of Central Intelligence; and

(3) Delegating authority to the various departments and agencies for research, development, procurement, and operation of designated means of collection.

(d) The foreign intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps, whose responsibilities shall include:

(1) Collection, production, and dissemination of military and military-related foreign intelligence and counterintelligence, and information on the foreign aspects of narcotics

production and trafficking. When collection is conducted in response to national foreign intelligence requirements, it will be conducted in accordance with guidance from the Director of Central Intelligence. Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI;

(2) Conduct of counterintelligence activities outside the United States in coordination with the CIA, and within the United States in coordination with the FBI; and

(3) Monitoring of the development, procurement, and management of tactical intelligence systems and equipment and conducting related research, development, and test and evaluation activities.

(e) Other offices within the Department of Defense appropriate for conduct of the intelligence missions and responsibilities assigned to the Secretary of Defense. If such other offices are used for intelligence purposes, the provisions of Part 2 of the Order shall apply to those offices when used for those purposes.

1.13 The Department of Energy. The Secretary of Energy shall:

(a) Participate with the Department of State in overtly collecting information with respect to foreign energy matters;

(b) Produce and disseminate foreign intelligence necessary for the Secretary's responsibilities;

(c) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(d) Provide expert technical, analytical, and research capability to other agencies within the Intelligence Community.

1.14 The Federal Bureau of Investigation. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the FBI shall:

(a) Within the United States conduct counterintelligence and coordinate counterintelligence activities of other agencies within the Intelligence Community. When a counterintelligence activity of the FBI involves military or civilian personnel of the Department of Defense, the FBI shall coordinate with the Department of Defense;

(b) Conduct counterintelligence activities outside the United States in coordination with the CIA as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General;

(c) Conduct within the United States, when required by the officials of the Intelligence Community designated by the President, activities undertaken to collect foreign intelligence or support foreign intelligence collection requirements of other agencies within the Intelligence Community, or, when requested by the Director of the National Security Agency, to support the communications security activities of the United States Government;

(d) Produce and disseminate foreign intelligence and counterintelligence; and

(e) Carry out or contract for research, development, and procurement of technical systems and devices relating to the functions authorized above.

PART 2 CONDUCT OF INTELLIGENCE ACTIVITIES

2.1 Need. Accurate and timely information about the capabilities, intentions, and activities of foreign powers, organizations, or persons and their agents is essential to informed decision-making in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 Purpose. This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable law, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of Information. Agencies within the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI or, when significant foreign intelligence is sought, by other authorized agencies of the Intelligence Community, provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other agencies of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence agencies. Contractors, or their present or former employees, or applicants for any such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contact for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.

2.4 Collection Techniques. Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The CIA to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by agencies other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when they are authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers, and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession.

(c) Physical surveillance of a United States person in the United States by agencies other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence agency contractors or their present or former employees, or applicants for any such employment of contracting; and

(2) Physical surveillance of a military person employed by a nonintelligence element of a military service.

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other methods.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with the Act, as well as this Order.

2.6 Assistance to Law Enforcement Authorities. Agencies within the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any agency within the Intelligence Community;

(b) Unless otherwise precluded by law or this Order, participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the General Counsel of the providing agency; and

(d) Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

2.7 Contracting. Agencies within the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contract or arrangements for authorized intelligence purposes. Contracts or arrangements width academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of agencies within the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any agency within the Intelligence Community without disclosing his intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such participation shall be authorized only it is essential to achieving lawful purpose as determined by the

agency head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 Human Experimentation. No agency within the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 Prohibition on Assassination. No person employed by or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination.

2.12 Indirect Participation. No agency of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

PART 3 GENERAL PROVISIONS

3.1 Congressional Oversight. The duties and responsibilities of the Director of Central Intelligence and the heads of other departments, agencies, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall be as provided in Title 50, United States Code, Section 413. The requirements of Section 662 of the Foreign Assistance Act of 1961, as amended (22 U.S.C. 2422) and Section 501 of the National Security Act of 1947, as amended (50 U.S.C. 413), shall apply to all special activities as defined in this Order.

3.2 Implementation. The NSC, the Secretary of Defense, the Attorney General, and the Director of Central Intelligence shall issue such appropriate directives and procedures as are necessary to implement this Order. Heads of agencies within the Intelligence Community shall issue appropriate supplementary directives and procedures consistent with this Order. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of any agency in the Intelligence Community other than the FBI. The National Security Council may establish procedures in instances where the agency head and the Attorney General are unable to reach agreement on other than constitutional or other legal grounds.

3.3 Procedures. Until the procedures required by this Order have been established, the activities herein authorized which require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order No. 12036. Procedures required by this Order shall be established as expeditiously as possible. All procedures promulgated pursuant to this Order shall be made available to the Congressional intelligence committees.

3.4 Definitions. For the purpose of this Order, the following terms shall have these meanings:

(a) Counterintelligence - means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of

foreign powers, organizations, or persons, or international terrorist activities but not including personnel, physical, document, or communications security programs.

(b) Electronic surveillance - means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(c) Employee - means a person employed by, assigned to, or acting for an agency within the Intelligence Community.

(d) Foreign Intelligence - means information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

(e) Intelligence Activities - means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to this Order.

(f) Intelligence Community and agencies within the Intelligence Community refer to the following agencies or organizations:

(1) The Central Intelligence Agency (CIA).

(2) The National Security Agency (NSC).

(3) The Defense Intelligence Agency (DIA).

(4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(5) The Bureau of Intelligence and Research of the Department of State;

(6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and

(7) The staff elements of the Director of Central Intelligence.

(g) The National Foreign Intelligence Program includes the programs listed below, but its composition shall be subject to review by the National Security Council and modification by the President:

(1) The programs of the CIA;

(2) The Consolidated Cryptologic Program, the General Defense Intelligence Program, and the programs of the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance, except such elements as the Director of Central Intelligence and the Secretary of Defense agree should be excluded;

(3) Other programs of agencies within the Intelligence Community designated jointly by the Director of Central Intelligence and the head of the department or by the President as national foreign intelligence or counterintelligence activities;

(4) Activities of the staff elements of the Director of Central Intelligence;

(5) Activities to acquire the intelligence required for the planning and conduct of tactical operations by the United States military forces are not included in the National Foreign Intelligence Program.

(h) Special activities - activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies, or media and do not include diplomatic activities or the collection and production of intelligence or related support functions.

(i) United States person - means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, and an organization incorporated in the United States except for a corporation directed and controlled by a foreign government or governments.

3.5 Purpose and Effect. This Order is intended to control and provide direction and guidance to the Intelligence Community. Nothing contained herein or in any procedures promulgated hereunder is intended to confer any substantive or procedural right or privilege on any person or organization.

3.6 Revocation. Executive Order No. 12036 of January 24, 1978, as amended, entitled "United States Intelligence Activities," is revoked.

RONALD REAGAN

THE WHITE HOUSE

December 4, 1981.

APPENDIX B

REPORT OF UNFAVORABLE INFORMATION OR SUSPENSION OF ACCESS

1. All reports of unfavorable information or suspension of access will be submitted on DA Form 5248-R, or in comparable message format (see Figure B-1).

2. DA Form 5248-R will be submitted in one copy to:

Commander US Army Central Personnel Security Clearance Facility ATTN: PCC-FP-RR Fort George G. Meade, Maryland 20755

3. If an immediate response is required, commanders may submit a report by message in DA Form 5248-R format to: CDRCCF FT MEADE MD//PCC-FP-RR//.

4. DA Form 5248-R will be completed as follows:

a. Block #1 - Reporting Commander Block: Proper mailing address, including attention line, zip code/APO, and Unit Identification Code (UIC) will be entered. Unit's or parent unit's USAIRR Requester Account Control Number will be entered in appropriate block.

b. Block #2 - Supporting Special Security Officer: Self explanatory.

c. Block #3 - Unit Identification Code: Enter the Unit Identification Code (UIC). The UIC will be that of current command/unit or the individual's new command/unit to which clearance results will be sent.

d. Block #4 - SSN: Enter Social Security Number.

e. Block #5a - Name: Last name of individual will be entered in CAPITAL letters, followed by first name and middle name, for example, SMITH, John James. Indicate: (NMN) - No middle name; (IO) - initial only; (NMI) no middle initial, as appropriate.

f. Block #5b - Aliases and Former Names: Indicate all former names, maiden names, nicknames, names changed by court order, and other names which Subject is or has been known by. If none, so state.

g. Block #6a - Birth Date: Enter year, month, and day of birth, for example, 79 JUN 15.

h. Block #6b - Birth Place: Self explanatory.

i. Block #7a - Rank or Grade: Enter military or civilian rank/grade, for example, SSG, PVT, GS-11.

j. Block #7b - Status: Indicate individual's current military or civilian status, for example, active duty military, Army National Guard, US Army Reserve, Department of the Army Civilian.

k. Block #8a - Current clearance: Enter level of security clearance appearing on DA Form 873.

l. Block #8b - SCI: Self explanatory.

m. Block #8c - Date Granted: This is based on Block #8b.

n. Block #8d - Date/Type of Investigation: This is based on Block #8b.

o. Block #9 - Type of Report: Enter either "Initial" or "Follow-up", or "Final." All first reports will be Initial reports.

p. Block #10 - Unit Action Taken: Enter any action taken by the commander, for example, "Access Suspended," "Access Not Suspended," or, in the case of a deserter or incarcerated individual, "Clearance Revoked - DA Form 873 attached."

q. Block #11a - Basis of Report Offense/Allegation:

(1) What was the prohibited substance possessed or used by the Subject?

(2) How was Subject's possession or use detected?

(3) Did the Subject ever possess or use the prohibited substance prior to this incident? If so, when and how frequently?

(4) What amount of prohibited substance is involved?

(5) What was/is Subject's frequency of use? (Specify in numbers.)

(6) Attempt to determine Subject's future intent concerning the use of prohibitive substances.

(7) Provide list of other offenses to include punishment(s).

r. Block #11b - Action Taken: Explain in detail the circumstances surrounding the basis for the report. Provide all amplifying information to enable an adjudicator to make a thorough and comprehensive security evaluation.

s. Block #11c - Cdr's Recommendations: Indicate actions by commander to have the derogatory information resolved, for example, "AR 15-6 initiated," LI requested for DIS," "CID requested to investigate," or "Commander's inquiry in progress."

t. Block #12 - Enclosures: Indicate and attach a copy of all investigations/inquiries.

u. Block #13 - Date: Self explanatory.

v. Block #14 - Signature, Typed Name, Rank, Title: Include typed or printed name and official title of the individual authorized to sign the request.

w. Block #15 - Signature of Security Manager/Authorized Official: Self explanatory.

x. Block #16 - Status Code: See Item 7b.

REPORT OF UNFAVORABLE INFORMATION FOR SECURITY DETERMINATION

For use of this form see AR 190-56; the proponent agency is ODCSOPS

1. REPORTING COMMANDER	2. SUPPORTING SPECIAL SECURITY OFFICE *(Sensitive Compartmented Information Only)*
3. UNIT IDENTIFICATION CODE	4. SOCIAL SECURITY NUMBER
5a. NAME *(Last, first, MI)*	5b. ALIASES *(Former/Maiden name)*

6a. DATE OF BIRTH *(Year, month, day)*	6b. PLACE OF BIRTH *(State or Country)*	7a. RANK	7b. STATUS *(see item 16)*

8a. CURRENT CLEARANCE	8b. SCI *(Check appropriate box)* ☐ YES ☐ NO	8c. DATE GRANTED	8d. DATE/TYPE OF INVESTIGATION

9. TYPE OF REPORT *(Check appropriate box)* ☐ INITIAL ☐ FOLLOW-UP ☐ FINAL

10. UNIT ACTION TAKEN *(Check appropriate box)*
☐ SCI ACCESS SUSPENDED ☐ ACCESS NOT SUSPENDED ☐ COLLATERAL ACCESS SUSPENDED *(873 Forwarded)*

11. BASIS OF REPORT

a. OFFENSE/ALLEGATION

b. ACTION TAKEN

c. CDR'S RECOMMENDATION

12. INCLOSURES

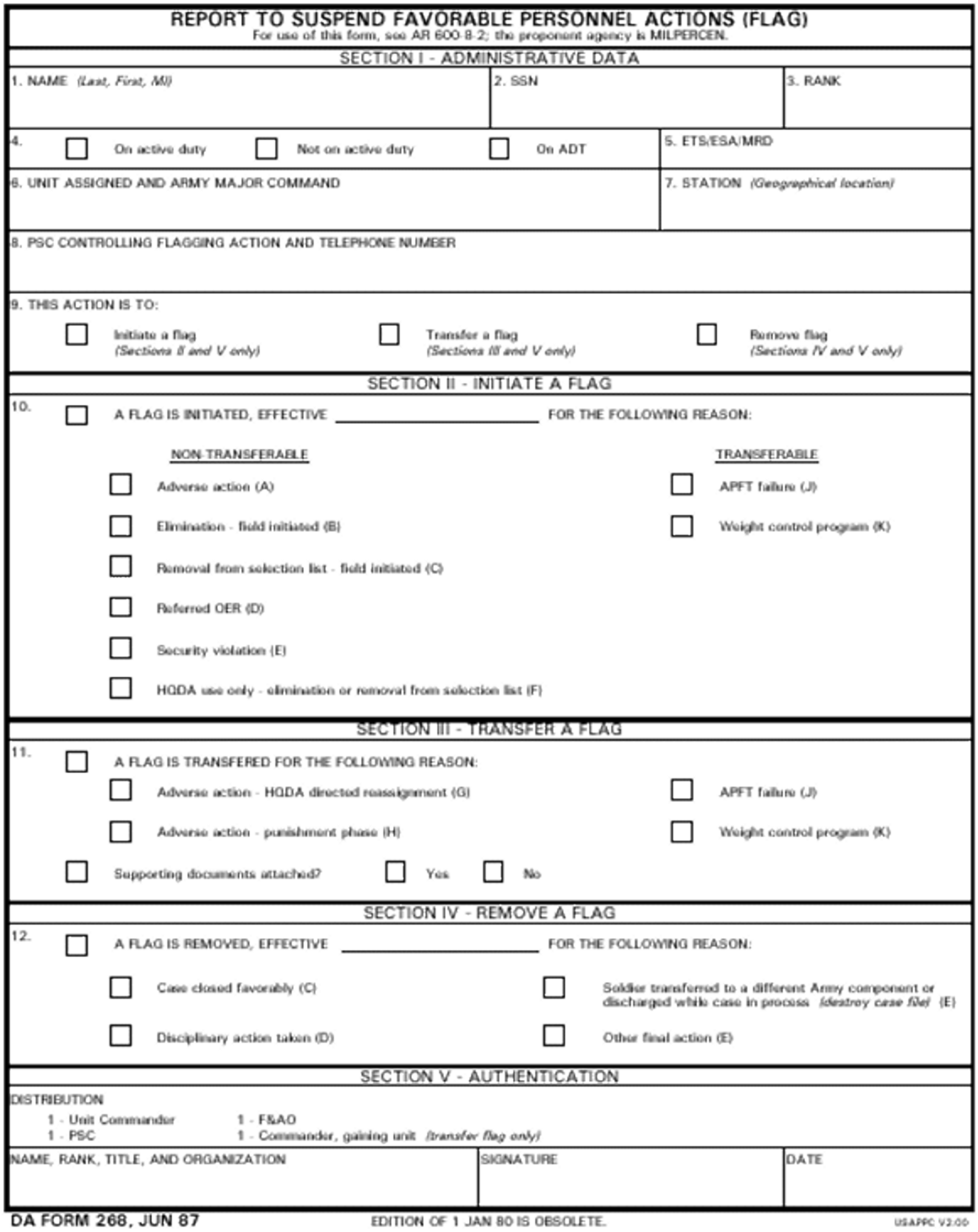
13. DATE	14. TYPED NAME, GRADE, TITLE, AND AUTOVON NO.	15. SIGNATURE OF SECURITY MANAGER/AUTHORIZED OFFICIAL

16. A - AAFES
C - DA CIVILIAN *(DAC)*
E - ACTIVE ENLISTED/OCS
F - NAF
G - ACTIVE GENERAL OFFICER
I - INACTIVE USAR
J - DAC AND ACTIVE USAR
K - DAC AND INACTIVE USAR
L - DAC AND ARNG
M - DAC AND DOD AFFILIATION
N - ARNG
O - ACTIVE OFFICER
R - ACTIVE USAR
S - SUMMER HIRE
T - CIVILIAN CONTRACTOR
W - ACTIVE WARRANT OFFICER
X - RED CROSS
Z - ROTC CADET
OTHER *(Explain)*

DA FORM 5248-R, SEP 83 USAPPC V1.00

Figure B-1.

APPENDIX C



REPORT TO SUSPEND FAVORABLE PERSONNEL ACTIONS (FLAG)
For use of this form, see AR 600-8-2; the proponent agency is MILPERCEN.

SECTION I - ADMINISTRATIVE DATA

1. NAME *(Last, First, MI)*	2. SSN	3. RANK

4. ☐ On active duty ☐ Not on active duty ☐ On ADT — 5. ETS/ESA/MRD

6. UNIT ASSIGNED AND ARMY MAJOR COMMAND — 7. STATION *(Geographical location)*

8. PSC CONTROLLING FLAGGING ACTION AND TELEPHONE NUMBER

9. THIS ACTION IS TO:

☐ Initiate a flag *(Sections II and V only)* ☐ Transfer a flag *(Sections III and V only)* ☐ Remove flag *(Sections IV and V only)*

SECTION II - INITIATE A FLAG

10. ☐ A FLAG IS INITIATED, EFFECTIVE _____ FOR THE FOLLOWING REASON:

NON-TRANSFERABLE

☐ Adverse action (A)
☐ Elimination - field initiated (B)
☐ Removal from selection list - field initiated (C)
☐ Referred OER (D)
☐ Security violation (E)
☐ HQDA use only - elimination or removal from selection list (F)

TRANSFERABLE

☐ APFT failure (J)
☐ Weight control program (K)

SECTION III - TRANSFER A FLAG

11. ☐ A FLAG IS TRANSFERED FOR THE FOLLOWING REASON:

☐ Adverse action - HQDA directed reassignment (G)
☐ Adverse action - punishment phase (H)
☐ APFT failure (J)
☐ Weight control program (K)

☐ Supporting documents attached? ☐ Yes ☐ No

SECTION IV - REMOVE A FLAG

12. ☐ A FLAG IS REMOVED, EFFECTIVE _____ FOR THE FOLLOWING REASON:

☐ Case closed favorably (C)
☐ Disciplinary action taken (D)
☐ Soldier transferred to a different Army component or discharged while case in process *(destroy case file)* (E)
☐ Other final action (E)

SECTION V - AUTHENTICATION

DISTRIBUTION
1 - Unit Commander 1 - F&AO
1 - PSC 1 - Commander, gaining unit *(transfer flag only)*

NAME, RANK, TITLE, AND ORGANIZATION	SIGNATURE	DATE

DA FORM 268, JUN 87 EDITION OF 1 JAN 80 IS OBSOLETE. USAPPC V2.00

APPENDIX D

DISCLOSURE ACCOUNTING RECORD		RECORD SYSTEM NAME AND TYPE			
INDIVIDUAL'S NAME	REQUESTER'S NAME AND ADDRESS	NATURE AND PURPOSE OF DISCLOSURE	INDIVIDUAL'S CONSENT (x)		DATE OF DISCLOSURE
			YES	NO	

Disclosure Accounting Record

RENDITION OF DA FORM 4410-R, 1 AUG 75

APPENDIX E

FREEDOM OF INFORMATION ACT *(FOIA)*/
OPERATIONS SECURITY *(OPSEC)* DESK TOP GUIDE

For use of this form, see AR 25-55; the proponent agency is ODISC4

Problem: The release of information from Department of the Army records must comply with the Freedom of Information Act *(FOIA)* and AR 25-55. At the same time, sensitive information concerning military operations and activities must be protected from disclosure to hostile intelligence services and their agents.

Solution: The following references to AR 25-55 and AR 530-1 outline proper policies and procedures.

Paragraph 5-200d, AR 25-55. Assigns areas of responsibility to the Initial Denial Authorities *(IDA)* for the Army. Only the Secretary of the Army and IDAs may deny a request for information submitted to the Army under the FOIA.

Paragraph 3-200, AR 25-55. Outlines the nine categories of records except from mandatory release under the FOIA. Denial under the exemptions is not automatic; each case must be reviewed and denial justified in each instance.

Paragraph 5-100c, AR 25-55. Discusses OPSEC considerations when reviewing information requested under the FOIA.

Paragraph 3-12, AR 530-1. Requires commanders to designate an OPSEC officer at battalion and higher levels of command to assist in discharging their responsibilities for Operations Security.

Paragraph 5-100d, AR 25-55. Invests command OPSEC points of contact with FOIA advisory functions. They will advise and assist FOIA personnel in dealing with requests for Information that have OPSEC implications.

CAUTION: Documents properly classified under Executive Order 12065 are automatically reviewed for operations security impact; however, the compilation of unclassified documents, or portions thereof, may combine information that, if released, might cause damage to national security *(para 2-211, AR 380-5)*. If you have any questions about releasing information, immediately contact your command OPSEC/FOIA advisor.

COMMAND OPSEC/FOIA ADVISOR	TELEPHONE NO.

DA FORM 4948-R, NOV 89 DA FORM 4948, APR 82 IS OBSOLETE USAPPC V1.01

APPENDIX F

PRIVACY ACT OF 1974

ADVISEMENT STATEMENT

US Army Intelligence is conducting an investigation of a counterintelligence matter, pursuant to Army regulations, which necessitates obtaining personal information from you. The Privacy Act of 1974, requires that each individual asked to provide personal information be advised of the following four points:

a. **AUTHORITY.** The Department of the Army (DA) is authorized to conduct counterintelligence investigations under Executive Order 10450, "Security Requirements for Government Employees," Executive Order 12333, "United States Intelligence Activities," and Title 10, United States Code, Section 3012.

b. **PRINCIPAL PURPOSES:** This investigation is being conducted by the Army to permit the responsible official(s) to determine the nature and extent of action, if any, necessary to ensure the security of the Army. The principal objectives in collecting this information are:

(1) To acquire factual information and/or evidence pertinent to the matter under investigation.

(2) To determine facts concerning possible compromise of US National Defense Information.

c. **ROUTINE USES.** The information obtained from you will become part of Army records and will be provided to those officials responsible for the security of the Army. The information may, at Army initiative or upon request, be furnished to accredited Department of Defense activities, other Federal agencies, and/or to law enforcement agencies for their official use. Under certain circumstances, pursuant to applicable international agreements, the information may be provided to security and/or law enforcement officials of a foreign government.

d. **VOLUNTARY OR MANDATORY NATURE OF DISCLOSURE.** The disclosure of personal information is voluntary. However, failure to disclose necessary and relevant information which impedes the investigation may have an adverse impact on your security clearance, if you possess or are being considered for one, or your employment, if you are a military member or employee of the Department of the Army.

SIGNATURE_____

DATE_____

DA FORM xx-R

APPENDIX G

DATA REQUIRED BY THE PRIVACY ACT OF 1974 (5 U.S.C. 552a)	
TITLE OF FORM	PRESCRIBING DIRECTIVE
1. AUTHORITY	
2. PRINICIPAL PURPOSE (S)	
3. ROUTINE USES	
4. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVDUAL NOT PROVIDING INFORMATION	
RENDITION OF DA FORM 4368-R PRIVACY ACT STATEMENT –25 SEP 75	

APPENDIX H

AARA	Access and Amendment Refusal Authority
ADP	Automatic Data Processing
BI	Background Investigation
CCF	US Central Personnel Security Clearance Facility
CI	Counterintelligence
CINCUSAEUR	Commander in Chief, US Army Europe
CTI	Complaint-type Investigation
DCSINT	Deputy Chief of Staff, Intelligence
DSS	Defense Security Service
EO	Executive Order
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FOIA	Freedom of Information Act
HQDA	Headquarters, Department of the Army
IDA	Initial Denial Authority
INSCOM	Intelligence and Security Command
IOSD	Intelligence Operations Support Detachment
KAWOL	Knowledgeable Personnel Absent Without Leave
LI	Limited Investigation
MAFOR	Military Absentees Known or Suspected of Having Gone to a Foreign Country or Embassy
MPRJ	Military Personnel Records Jacket
NAC	National Agency Check
NSA	National Security Agency
ODCSINT	Office of Deputy Chief of Staff, Intelligence (see DCSINT, DA)
OMPF	Official Military Personnel File
OPLAN	Operations Plan
OPSEC	Operations Security
OSE	Operations Security Evaluation
PAC	Personnel and Administration Center
PCCF	Personnel Center Clearance Facility

PSI	Personnel Security Investigation
SAEDA	Subversion and Espionage Directed Against the Army
SCI	Sensitive Compartmented Information
SSN	Social Security Number
UCMJ	Uniform Code of Military Justice
USACIDC	US Army Criminal Investigation Command
USAIRR	US Army Investigative Records Repository
USC	United States Code